НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2026-09-23.1 | 23 сентября 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-65810	.NET	Локальный	PE	2026-08-18	✓
2	Критическая	CVE-2026-39831	Go	Сетевой	OSI	2026-08-18	✓
3	Критическая	CVE-2026-39834	Go	Сетевой	DoS	2026-08-18	✓
4	Критическая	CVE-2026-39833	Go	Сетевой	OSI	2026-08-18	✓
5	Высокая	CVE-2026-62737	Windows Kernel	Локальный	DoS	2026-08-18	✓
6	Высокая	CVE-2026-47301	Microsoft Configuration Manager	Сетевой	PE	2026-08-18	✓
7	Высокая	CVE-2026-69414	Microsoft Defender	Локальный	PE	2026-08-19	✓
8	Высокая	CVE-2026-14669	PostgreSQL	Сетевой	ACE	2026-08-17	✓
9	Высокая	CVE-2026-53413	Zoom	Сетевой	ACE	2026-08-18	✓
10	Высокая	CVE-2026-74883	openssl_encrypt	Сетевой	ACE	2026-08-18	✓
11	Критическая	BDU:2026-11902	GeoServer	Сетевой	ACE	2026-08-19	✓
12	Высокая	CVE-2026-48438	Content Credentials JS SDK	Сетевой	DoS	2026-08-12	✓
13	Высокая	CVE-2026-48439	Content Credentials JS SDK	Сетевой	DoS	2026-08-12	✓

14	Критическая	CVE-2026-74251	Joomla Phoca Cart	Сетевой	OSI	2026-08-19	✓
15	Высокая	CVE-2026-18408	PostgreSQL	Сетевой	ACE	2026-08-17	✓
16	Высокая	CVE-2026-19385	PostgreSQL	Сетевой	ACE	2026-08-17	✓
17	Высокая	CVE-2026-6464	PostgreSQL	Сетевой	ACE	2026-08-17	✓
18	Высокая	CVE-2026-16239	PostgreSQL	Сетевой	ACE	2026-08-17	✓
19	Высокая	CVE-2026-66046	Expat	Сетевой	DoS	2026-08-19	✓
20	Высокая	CVE-2026-16238	PostgreSQL	Сетевой	ACE	2026-08-17	✓
21	Высокая	CVE-2026-14676	PostgreSQL	Сетевой	ACE	2026-08-17	✓
22	Высокая	CVE-2026-15741	PostgreSQL	Сетевой	ACE	2026-08-17	✓
23	Высокая	CVE-2026-14662	PostgreSQL	Сетевой	ACE	2026-08-17	✓
24	Высокая	CVE-2026-15742	PostgreSQL	Сетевой	ACE	2026-08-17	✓
25	Высокая	CVE-2026-14668	PostgreSQL	Сетевой	OSI	2026-08-17	✓
26	Высокая	CVE-2026-14670	PostgreSQL	Сетевой	ACE	2026-08-17	✓
27	Высокая	CVE-2026-14664	PostgreSQL	Сетевой	ACE	2026-08-17	✓
28	Высокая	CVE-2026-14677	PostgreSQL	Сетевой	ACE	2026-08-17	✓

29	Высокая	CVE-2026-14679	PostgreSQL	Сетевой	ACE	2026-08-17	✓
30	Высокая	CVE-2026-14680	PostgreSQL	Сетевой	ACE	2026-08-17	✓
31	Высокая	CVE-2026-14671	PostgreSQL	Сетевой	ACE	2026-08-17	✓
32	Высокая	CVE-2026-24451	Gitea	Сетевой	OSI	2026-08-19	✓
33	Критическая	CVE-2026-42535	Apache HTTP Server	Сетевой	OSI	2026-08-20	✓
34	Высокая	CVE-2026-47303	ASP.NET Core	Сетевой	PE	2026-08-20	✓
35	Высокая	CVE-2026-47300	ASP.NET Core	Сетевой	SB	2026-08-20	✓
36	Высокая	CVE-2026-26018	CoreDNS	Сетевой	PE	2026-08-19	✓
37	Высокая	CVE-2026-75918	phpMyFAQ	Сетевой	OSI	2026-08-21	✓
38	Критическая	CVE-2026-64849	MLflow	Сетевой	RLF	2026-08-20	✓
39	Критическая	CVE-2026-72898	Metabase	Сетевой	ACE	2026-08-21	✓
40	Высокая	CVE-2026-46326	Linux	Локальный	DoS	2026-08-20	✓
41	Высокая	CVE-2026-45938	Linux	Смежная сеть	DoS	2026-08-20	✓
42	Критическая	CVE-2026-45898	Linux	Сетевой	DoS	2026-08-20	✓
43	Высокая	CVE-2026-31717	Linux	Сетевой	DoS	2026-08-20	✓

44	Высокая	CVE-2026-44252	Wazuh	Сетевой	PE	2026-08-21	✓
45	Критическая	CVE-2026-49441	Wazuh	Сетевой	ACE	2026-08-21	✓
46	Критическая	CVE-2026-48024	Wazuh	Сетевой	ACE	2026-08-21	✓
47	Высокая	CVE-2026-76928	Wireshark	Сетевой	DoS	2026-08-24	✓
48	Высокая	CVE-2026-76208	phpMyFAQ	Сетевой	CI	2026-08-21	✓
49	Высокая	CVE-2026-76207	phpMyFAQ	Сетевой	OSI	2026-08-21	✓
50	Высокая	CVE-2026-76205	phpMyFAQ	Сетевой	OSI	2026-08-21	✓
51	Высокая	CVE-2026-76879	Wireshark	Сетевой	DoS	2026-08-24	✓
52	Высокая	CVE-2026-76886	Wireshark	Сетевой	DoS	2026-08-24	✓
53	Критическая	CVE-2026-69836	Microsoft Entra ID	Сетевой	ACE	2026-08-24	✓
54	Высокая	CVE-2026-40622	Unbound	Сетевой	OSI	2026-08-18	✓
55	Высокая	CVE-2026-33489	CoreDNS	Сетевой	OSI	2026-08-20	✓
56	Высокая	CVE-2026-33190	CoreDNS	Сетевой	SB	2026-08-19	✓
57	Высокая	CVE-2026-32936	CoreDNS	Сетевой	DoS	2026-08-19	✓
58	Высокая	CVE-2026-32934	CoreDNS	Сетевой	DoS	2026-08-19	✓

59	Высокая	CVE-2026-32740	Libheif	Сетевой	ACE	2026-08-19	✓
60	Высокая	CVE-2026-76219	GitPython	Сетевой	OAF	2026-08-21	✓
61	Высокая	CVE-2026-76220	GitPython	Сетевой	ACE	2026-08-21	✓
62	Высокая	CVE-2026-76222	GitPython	Сетевой	OAF	2026-08-21	✓
63	Высокая	CVE-2026-76221	GitPython	Сетевой	ACE	2026-08-21	✓
64	Критическая	CVE-2026-43125	Linux	Сетевой	ACE	2026-07-27	✓
65	Критическая	CVE-2026-43383	Linux	Сетевой	ACE	2026-07-27	✓
66	Критическая	CVE-2026-43198	Linux	Сетевой	ACE	2026-07-27	✓
67	Критическая	CVE-2026-43407	Linux	Сетевой	DoS	2026-07-27	✓
68	Критическая	CVE-2026-43117	Linux	Сетевой	DoS	2026-07-27	✓
69	Критическая	CVE-2026-43197	Linux	Сетевой	DoS	2026-07-27	✓
70	Критическая	CVE-2026-43406	Linux	Сетевой	DoS	2026-07-27	✓
71	Критическая	CVE-2026-43083	Linux	Сетевой	DoS	2026-07-27	✓
72	Высокая	CVE-2026-31476	Linux	Сетевой	DoS	2026-08-18	✓
73	Критическая	CVE-2026-31501	Linux	Сетевой	ACE	2026-08-18	✓

74	Высокая	CVE-2026-31513	Linux	Смежная сеть	DoS	2026-08-18	✓
75	Высокая	CVE-2026-31396	Linux	Смежная сеть	ACE	2026-08-13	✓
76	Высокая	CVE-2026-23424	Linux	Смежная сеть	ACE	2026-08-13	✓
77	Критическая	CVE-2026-31536	Linux	Сетевой	ACE	2026-08-18	✓
78	Критическая	CVE-2026-23427	Linux	Сетевой	ACE	2026-08-13	✓
79	Критическая	CVE-2026-23428	Linux	Сетевой	ACE	2026-08-19	✓
80	Высокая	CVE-2026-23432	Linux	Смежная сеть	ACE	2026-08-13	✓
81	Высокая	CVE-2026-23446	Linux	Смежная сеть	ACE	2026-08-13	✓
82	Высокая	CVE-2026-23459	Linux	Сетевой	OAF	2026-08-19	✓
83	Критическая	CVE-2026-31405	Linux	Сетевой	ACE	2026-08-19	✓
84	Высокая	CVE-2026-31412	Linux	Смежная сеть	ACE	2026-08-19	✓
85	Высокая	CVE-2026-31417	Linux	Смежная сеть	ACE	2026-08-19	✓
86	Высокая	CVE-2026-31433	Linux	Сетевой	ACE	2026-08-18	✓

87	Критическая	CVE-2026-31463	Linux	Сетевой	ACE	2026-08-18	✓
88	Высокая	CVE-2026-31553	Linux	Локальный	ACE	2026-08-18	✓
89	Критическая	CVE-2026-31659	Linux	Сетевой	ACE	2026-08-18	✓
90	Критическая	CVE-2026-77413	JSONata	Сетевой	ACE	2026-08-25	✓
91	Критическая	CVE-2026-77414	JSONata	Сетевой	ACE	2026-08-25	✓
92	Критическая	CVE-2026-77415	JSONata	Сетевой	ACE	2026-08-25	✓
93	Высокая	CVE-2026-31558	Linux	Локальный	ACE	2026-08-18	✓
94	Критическая	CVE-2026-31608	Linux	Сетевой	ACE	2026-08-18	✓
95	Высокая	CVE-2026-31611	Linux	Сетевой	ACE	2026-08-18	✓
96	Высокая	CVE-2026-31613	Linux	Сетевой	DoS	2026-08-21	✓
97	Высокая	CVE-2026-23372	Linux	Смежная сеть	ACE	2026-08-11	✓
98	Высокая	CVE-2026-31788	Linux	Локальный	ACE	2026-08-07	✓
99	Высокая	CVE-2026-23395	Linux	Смежная сеть	ACE	2026-08-11	✓
100	Критическая	CVE-2026-31414	Linux	Сетевой	ACE	2026-08-19	✓
101	Высокая	CVE-2026-23456	Linux	Сетевой	OSI	2026-08-18	✓

102	Критическая	CVE-2026-23455	Linux	Сетевой	ACE	2026-08-13	✓
103	Высокая	CVE-2026-31631	Linux	Сетевой	OSI	2026-08-18	✓
104	Высокая	CVE-2026-31464	Linux	Смежная сеть	DoS	2026-08-18	✓
105	Критическая	CVE-2026-31448	Linux	Сетевой	ACE	2026-08-18	✓
106	Критическая	CVE-2026-31636	Linux	Сетевой	DoS	2026-08-18	✓
107	Высокая	CVE-2026-31435	Linux	Сетевой	ACE	2026-08-18	✓
108	Высокая	CVE-2026-31570	Linux	Смежная сеть	ACE	2026-08-18	✓
109	Критическая	CVE-2026-31609	Linux	Сетевой	ACE	2026-08-18	✓
110	Критическая	CVE-2026-31633	Linux	Сетевой	ACE	2026-08-18	✓
111	Критическая	CVE-2026-31637	Linux	Сетевой	ACE	2026-08-18	✓
112	Критическая	CVE-2026-31649	Linux	Сетевой	ACE	2026-08-18	✓
113	Высокая	CVE-2026-31392	Linux	Локальный	ACE	2026-08-18	✓
114	Критическая	CVE-2026-31436	Linux	Сетевой	ACE	2026-08-18	✓
115	Критическая	CVE-2026-31607	Linux	Сетевой	ACE	2026-08-18	✓

116	Высокая	CVE-2026-31393	Linux	Смежная сеть	OAF	2026-08-19	✓
117	Высокая	CVE-2026-23280	Linux	Смежная сеть	ACE	2026-08-11	✓
118	Высокая	CVE-2026-23281	Linux	Смежная сеть	ACE	2026-08-11	✓
119	Высокая	CVE-2026-23457	Linux	Сетевой	OSI	2026-08-19	✓
120	Высокая	CVE-2026-63388	Libevent	Локальный	DoS	2026-08-26	✓
121	Критическая	CVE-2026-43384	Linux	Сетевой	ACE	2026-07-27	✓
122	Критическая	CVE-2026-43414	Linux	Сетевой	ACE	2026-07-27	✓
123	Высокая	CVE-2026-73570	Zimbra Collaboration Suite	Сетевой	ACE	2026-08-26	✓
124	Высокая	CVE-2026-63495	Libevent	Сетевой	DoS	2026-08-25	✓
125	Критическая	CVE-2026-63385	Libevent	Сетевой	DoS	2026-08-26	✓
126	Критическая	CVE-2026-43465	Linux	Сетевой	ACE	2026-07-27	✓
127	Высокая	CVE-2026-63383	Libevent	Сетевой	DoS	2026-08-26	✓
128	Критическая	CVE-2026-63382	Libevent	Сетевой	DoS	2026-08-26	✓
129	Высокая	CVE-2026-55553	urllib	Сетевой	OSI	2026-08-26	✓

130	Высокая	CVE-2026-63384	Libevent	Сетевой	DoS	2026-08-26	✓
131	Высокая	CVE-2026-78675	GitPython	Локальный	ACE	2026-08-26	✓
132	Критическая	CVE-2026-42990	SQL Server ODBC driver	Сетевой	PE	2026-08-26	✓
133	Высокая	CVE-2026-42975	Windows Bluetooth Port Driver	Смежная сеть	ACE	2026-08-26	✓
134	Высокая	CVE-2026-43426	Linux	Смежная сеть	ACE	2026-07-28	✓
135	Высокая	CVE-2026-42982	Windows Secure Kernel Mode	Локальный	PE	2026-08-26	✓
136	Высокая	CVE-2026-43318	Linux	Смежная сеть	ACE	2026-07-28	✓
137	Высокая	CVE-2026-43185	Linux	Сетевой	ACE	2026-07-28	✓
138	Высокая	CVE-2026-43098	Linux	Смежная сеть	ACE	2026-07-28	✓
139	Высокая	CVE-2026-43380	Linux	Смежная сеть	ACE	2026-07-28	✓
140	Высокая	CVE-2026-43376	Linux	Сетевой	ACE	2026-07-28	✓
141	Высокая	CVE-2026-77354	kin-openapi	Сетевой	DoS	2026-08-26	✓
142	Высокая	CVE-2026-43460	Linux	Смежная сеть	ACE	2026-07-28	✓
143	Высокая	CVE-2026-76905	kin-openapi	Сетевой	DoS	2026-08-26	✓

144	Высокая	CVE-2026-73939	Helidon	Сетевой	ACE	2026-08-20	✓
145	Критическая	CVE-2026-78676	GitPython	Сетевой	ACE	2026-08-26	✓
146	Высокая	CVE-2026-61798	Netty	Сетевой	OSI	2026-08-26	✓
147	Высокая	CVE-2026-73931	Helidon	Сетевой	DoS	2026-08-20	✓
148	Высокая	CVE-2026-73929	Helidon	Сетевой	DoS	2026-08-20	✓
149	Высокая	CVE-2026-73927	Helidon	Сетевой	DoS	2026-08-20	✓
150	Высокая	CVE-2026-73925	Helidon	Сетевой	ACE	2026-08-20	✓
151	Критическая	CVE-2026-73924	Helidon	Сетевой	ACE	2026-08-20	✓
152	Критическая	CVE-2026-73922	Helidon	Сетевой	ACE	2026-08-20	✓
153	Критическая	CVE-2026-73921	Helidon	Сетевой	ACE	2026-08-20	✓
154	Критическая	CVE-2026-73920	Helidon	Сетевой	DoS	2026-08-20	✓
155	Критическая	CVE-2026-73917	Helidon	Сетевой	ACE	2026-08-20	✓
156	Критическая	CVE-2026-73930	Helidon	Сетевой	DoS	2026-08-20	✓
157	Высокая	CVE-2026-73934	Helidon	Сетевой	DoS	2026-08-20	✓
158	Высокая	CVE-2026-73935	Helidon	Сетевой	DoS	2026-08-20	✓

159	Высокая	CVE-2026-73936	Helidon	Сетевой	DoS	2026-08-20	✓
160	Высокая	CVE-2026-73937	Helidon	Сетевой	DoS	2026-08-20	✓
161	Высокая	CVE-2026-73938	Helidon	Сетевой	OSI	2026-08-20	✓
162	Высокая	CVE-2026-78677	GitPython	Сетевой	WLF	2026-08-26	✓
163	Критическая	CVE-2026-76904	GeoTools	Сетевой	ACE	2026-08-27	✓
164	Критическая	CVE-2026-79657	Python NLTK library	Сетевой	ACE	2026-08-26	✓
165	Высокая	CVE-2026-78682	Python NLTK library	Сетевой	RLF	2026-08-26	✓
166	Критическая	CVE-2026-73916	Helidon	Сетевой	ACE	2026-08-20	✓
167	Высокая	CVE-2026-31563	Linux	Сетевой	DoS	2026-08-28	✓
168	Высокая	CVE-2026-34253	vorbis-tools	Сетевой	DoS	2026-08-28	✓
169	Высокая	CVE-2026-31779	Linux	Смежная сеть	DoS	2026-08-28	✓
170	Высокая	CVE-2026-43402	Linux	Локальный	ACE	2026-07-29	✓
171	Высокая	CVE-2026-62792	Windows TCP/IP	Сетевой	ACE	2026-08-27	✓
172	Высокая	CVE-2026-62770	Windows Shell	Локальный	PE	2026-08-27	✓
173	Высокая	CVE-2026-62721	Windows User-Mode Power Service	Локальный	PE	2026-08-27	✓

174	Высокая	CVE-2026-61355	Windows Sensor Data Service	Локальный	PE	2026-08-27	✓
175	Высокая	CVE-2026-61358	Windows Accessibility Infrastructure	Локальный	PE	2026-08-27	✓
176	Высокая	CVE-2026-61363	Remote Desktop Client	Сетевой	ACE	2026-08-27	✓
177	Высокая	CVE-2026-62710	Windows Device Association Service	Локальный	PE	2026-08-27	✓
178	Высокая	CVE-2026-62711	Windows Win32k	Локальный	PE	2026-08-27	✓
179	Высокая	CVE-2026-62781	RPC Runtime Library	Сетевой	ACE	2026-08-27	✓
180	Высокая	CVE-2026-62797	Windows NTFS	Локальный	PE	2026-08-27	✓
181	Высокая	CVE-2026-62876	Windows Win32k	Локальный	PE	2026-08-27	✓
182	Высокая	CVE-2026-68816	Microsoft Excel	Локальный	ACE	2026-08-27	✓
183	Высокая	CVE-2026-20313	Catalyst SD-WAN Manager	Сетевой	DoS	2026-08-28	✓
184	Высокая	CVE-2026-68801	Microsoft Excel	Локальный	ACE	2026-08-27	✓
185	Высокая	CVE-2026-20312	Catalyst SD-WAN Manager	Сетевой	ACE	2026-08-28	✓
186	Высокая	CVE-2026-79674	Python NLTK library	Сетевой	OSI	2026-08-28	✓
187	Критическая	CVE-2026-56291	Balbooa Forms	Сетевой	ACE	2026-08-31	✓
188	Высокая	CVE-2026-43208	Linux	Сетевой	ACE	2026-07-29	✓

189	Критическая	BDU:2026-13254	DIAFAN.CMS	Сетевой	ACE	2026-08-31	✓
190	Критическая	CVE-2026-72137	Linux	Сетевой	ACE	2026-08-31	✓
191	Высокая	CVE-2026-70463	Rsync	Сетевой	SB	2026-08-31	✓
192	Высокая	CVE-2026-77368	SeaweedFS	Сетевой	SB	2026-08-31	✓
193	Высокая	CVE-2026-65681	Windows iSCSI Target Service	Сетевой	DoS	2026-09-01	✓
194	Высокая	CVE-2026-62889	Windows Secure Socket Tunneling Protocol	Сетевой	ACE	2026-09-01	✓
195	Высокая	CVE-2026-65679	Windows iSCSI Target Service	Сетевой	ACE	2026-09-01	✓
196	Высокая	CVE-2026-65671	Remote Access API	Локальный	PE	2026-09-01	✓
197	Высокая	CVE-2026-62888	Windows DWM Core Library	Локальный	PE	2026-09-01	✓
198	Высокая	CVE-2026-62890	Windows GDI+	Локальный	PE	2026-09-01	✓
199	Высокая	CVE-2026-62816	Windows Reliable Multicast Transport Driver	Смежная сеть	ACE	2026-09-01	✓
200	Высокая	CVE-2026-62824	Remote Desktop Client	Сетевой	ACE	2026-09-01	✓
201	Высокая	CVE-2026-62820	Windows DNS Server	Сетевой	ACE	2026-09-01	✓
202	Высокая	CVE-2026-62818	Windows Active Directory Certificate Services	Сетевой	ACE	2026-09-01	✓

203	Высокая	CVE-2026-62817	Windows DNS Server	Смежная сеть	ACE	2026-09-01	✓
204	Высокая	CVE-2026-65787	Desktop Window Manager	Локальный	PE	2026-09-01	✓
205	Критическая	CVE-2026-62878	Windows DNS Server	Сетевой	ACE	2026-09-01	✓
206	Высокая	CVE-2026-65789	Windows DNS Server	Сетевой	ACE	2026-09-01	✓
207	Высокая	CVE-2026-71331	Windows Device Health Attestation	Сетевой	ACE	2026-09-01	✓
208	Высокая	CVE-2026-65790	Windows Message Queuing	Локальный	PE	2026-09-01	✓
209	Высокая	CVE-2026-65814	Microsoft Windows Storage Port Driver	Локальный	PE	2026-09-01	✓
210	Критическая	CVE-2026-55068	NRF RegisterNFInstance	Сетевой	OSI	2026-08-31	✓
211	Критическая	CVE-2026-55220	PHP pimcore	Сетевой	ACE	2026-08-31	✓
212	Высокая	CVE-2026-55245	Bifrost	Сетевой	RLF	2026-08-31	✓
213	Высокая	CVE-2026-82254	gix-pack	Сетевой	DoS	2026-09-01	✓
214	Высокая	BDU:2026-13271	Apache Log4j Core	Сетевой	ACE	2026-09-01	✓
215	Высокая	BDU:2026-13272	Avast Antivirus	Локальный	PE	2026-09-01	✓
216	Высокая	CVE-2026-82457	su-exec	Локальный	ACE	2026-08-31	✓
217	Высокая	CVE-2026-70346	Windows Installer	Локальный	PE	2026-09-01	✓

218	Высокая	CVE-2026-70347	Windows Installer	Локальный	PE	2026-09-01	✓
219	Высокая	CVE-2026-66802	Windows Device Health Attestation	Сетевой	ACE	2026-09-01	✓
220	Высокая	CVE-2026-66799	Windows Key Guard	Локальный	PE	2026-09-01	✓
221	Критическая	CVE-2026-65791	Windows iSCSI Target Service	Сетевой	ACE	2026-09-01	✓
222	Высокая	CVE-2026-66804	Microsoft Windows Cross Device Service	Локальный	PE	2026-09-01	✓
223	Критическая	CVE-2026-35579	CoreDNS	Сетевой	PE	2026-08-24	✓
224	Критическая	CVE-2026-41551	ROS#	Сетевой	ACE	2026-05-13	✓
225	Высокая	CVE-2026-81891	elFinder	Сетевой	ACE	2026-09-02	✓
226	Высокая	CVE-2026-81889	elFinder	Сетевой	OSI	2026-09-02	✓
227	Высокая	CVE-2026-63072	OpenSSL	Сетевой	DoS	2026-09-02	✓
228	Высокая	CVE-2026-62911	Microsoft Exchange Server	Сетевой	PE	2026-09-02	✓
229	Высокая	CVE-2026-62388	Python NLTK library	Сетевой	SB	2026-09-02	✓
230	Критическая	CVE-2026-77806	SPIP	Сетевой	ACE	2026-09-02	✓
231	Критическая	CVE-2026-54350	Budibase	Сетевой	ACE	2026-09-02	✓
232	Высокая	CVE-2026-62807	Windows DHCP Server	Локальный	PE	2026-09-02	✓

233	Высокая	CVE-2026-62812	Windows DHCP Server	Локальный	PE	2026-09-02	✓
234	Критическая	CVE-2026-62893	Windows Deployment Services TFTP Server	Сетевой	ACE	2026-09-02	✓
235	Высокая	CVE-2026-62803	Windows DHCP Server	Локальный	PE	2026-09-02	✓
236	Высокая	CVE-2026-66393	Python NLTK library	Сетевой	DoS	2026-09-02	✓
237	Высокая	CVE-2026-80724	Linux	Локальный	ACE	2026-09-02	✓
238	Высокая	CVE-2026-83618	XMLDOM	Сетевой	LoI	2026-09-02	✓
239	Высокая	CVE-2026-83619	XMLDOM	Сетевой	DoS	2026-09-02	✓
240	Высокая	CVE-2026-83617	XMLDOM	Сетевой	SB	2026-09-02	✓
241	Высокая	CVE-2026-83612	XMLDOM	Сетевой	DoS	2026-09-02	✓
242	Высокая	CVE-2026-63520	Microsoft SharePoint Server	Сетевой	ACE	2026-09-03	✓
243	Критическая	CVE-2026-48020	Traefik	Сетевой	SB	2026-09-03	✓
244	Высокая	CVE-2026-84189	LibreNMS	Сетевой	XSS\CSS	2026-09-02	✓
245	Высокая	CVE-2026-53202	Linux	Локальный	ACE	2026-08-28	✓
246	Высокая	CVE-2026-53635	Open edX Platform	Сетевой	RLF	2026-09-04	✓
247	Высокая	CVE-2026-53636	Open edX Platform	Сетевой	SB	2026-09-04	✓

248	Критическая	CVE-2026-53221	Linux	Сетевой	ACE	2026-08-28	✓
249	Высокая	CVE-2026-85046	Google Chrome	Сетевой	ACE	2026-09-04	✓
250	Высокая	CVE-2026-53226	Linux	Смежная сеть	ACE	2026-08-28	✓
251	Критическая	CVE-2026-53228	Linux	Сетевой	ACE	2026-08-28	✓
252	Высокая	CVE-2026-53240	Linux	Сетевой	ACE	2026-08-28	✓
253	Критическая	CVE-2026-53246	Linux	Сетевой	ACE	2026-08-28	✓
254	Критическая	CVE-2026-53225	Linux	Сетевой	DoS	2026-08-28	✓
255	Критическая	CVE-2026-53176	Linux	Сетевой	ACE	2026-08-28	✓
256	Высокая	CVE-2026-53178	Linux	Смежная сеть	DoS	2026-08-27	✓
257	Критическая	CVE-2026-53175	Linux	Сетевой	ACE	2026-08-28	✓
258	Высокая	CVE-2026-53170	Linux	Локальный	ACE	2026-08-28	✓
259	Высокая	CVE-2026-53159	Linux	Локальный	ACE	2026-08-28	✓
260	Критическая	CVE-2026-53260	Linux	Сетевой	ACE	2026-08-28	✓
261	Высокая	CVE-2026-53266	Linux	Локальный	ACE	2026-08-28	✓
262	Критическая	CVE-2026-26035	FortiWeb	Сетевой	SB	2026-08-26	✓

263	Критическая	BDU:2026-14138	Atlassian Confluence	Сетевой	PE	2026-09-04	✓

1

Краткое описание: Повышение привилегий в .NET

Идентификатор уязвимости: CVE-2026-65810
BDU:2026-11944

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

Уязвимый продукт: Windows 10 1607: -
Windows 10 1809: -
Windows 10 21H2: -
Windows 10 22H2: -
Windows 11 23H2: -
Windows 11 24H2: -
Windows Server 2012: -
Windows Server 2012 R2: -
Windows Server 2012 (Server Core installation): -
Windows Server 2012 R2 (Server Core installation): -
Windows Server 2016: -
Windows Server 2016 (Server Core installation): -
Windows Server 2019: -
Windows Server 2019 (Server Core installation): -
Windows Server 2022: -
Windows Server 2022 (Server Core installation): -
Windows Server 2025: -
Windows Server 2025 (Server Core installation): -
Microsoft .NET Framework 3.5: до 4.8.9343.0
Microsoft .NET Framework 4.6.2: до 4.7.4144.0
Microsoft .NET Framework 4.7: до 4.7.4144.0
Microsoft .NET Framework 4.7.1: до 4.7.4144.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.8980
Microsoft .NET Framework 4.8: до 3.0.30729.9169
Microsoft .NET Framework 4.8.1: до 4.8.9343.0
Windows 11 25H2: -
Windows 11 26H1: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65810
- https://bdu.fstec.ru/vul/2026-11944

2

Краткое описание: Получение конфиденциальной информации в Go

Идентификатор уязвимости: CVE-2026-39831
BDU:2026-11948

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Go: до 0.52.0
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5019
- https://groups.google.com/g/golang-announce/c/a082jnz-LvI
- https://github.com/golang/go/issues/79566
- https://go-review.googlesource.com/c/crypto/+/781662
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-11948

3

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-39834
BDU:2026-11949

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Go: до 0.52.0
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5020
- https://go.dev/cl/781662
- https://go.dev/issue/79566
- https://groups.google.com/g/golang-announce/c/a082jnz-LvI
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-11949

4

Краткое описание: Получение конфиденциальной информации в Go

Идентификатор уязвимости: CVE-2026-39833
BDU:2026-11950

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Go: до 0.52.0
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5005
- https://go.dev/issue/79436
- https://go.dev/cl/778642
- https://groups.google.com/g/golang-announce/c/a082jnz-LvI
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-11950

5

Краткое описание: Отказ в обслуживании в Windows Kernel

Идентификатор уязвимости: CVE-2026-62737
BDU:2026-11889

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.9106
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://github.com/loanvui/CVE-2026-62737
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62737
- https://www.helpnetsecurity.com/2026/08/12/august-2026-patch-tuesday-cve-2026-68820/
- https://github.com/DavidCarliez/cve-2026-62737-lab
- https://bdu.fstec.ru/vul/2026-11889

6

Краткое описание: Повышение привилегий в Microsoft Configuration Manager

Идентификатор уязвимости: CVE-2026-47301
BDU:2026-11890

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Configuration Manager 2503: до 5.0.9135.1031
Microsoft Configuration Manager 2603: до 5.0.9146.1021
Microsoft Configuration Manager 2509: до 5.0.9141.1030

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47301
- https://github.com/OmriBaso/SCCM-CVE-2026-47301-Remote-Code-Execution-Exploit
- https://bdu.fstec.ru/vul/2026-11890

7

Краткое описание: Повышение привилегий в Microsoft Defender

Идентификатор уязвимости: CVE-2026-69414
BDU:2026-11893

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Malware Protection Engine: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69414
- https://github.com/1neptune/ShieldBreak
- https://bdu.fstec.ru/vul/2026-11893

8

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14669
BDU:2026-11894

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14669
- https://github.com/HackSpeak/CVE-2026-14669
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11894

9

Краткое описание: Выполнение произвольного кода в Zoom

Идентификатор уязвимости: CVE-2026-53413
BDU:2026-11898

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Zoom Video SDK: до 2.6.0
Zoom Rooms: до 7.1.0
Zoom Meeting SDK: до 7.1.0
Zoom Workplace Desktop App: до 7.0.6
Zoom Workplace VDI Client for Windows: до 6.6.16

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.zoom.com/en/trust/security-bulletin/zsb-26015/
- https://github.com/HORKimhab/CVE-2026-53413
- https://bdu.fstec.ru/vul/2026-11898

10

Краткое описание: Выполнение произвольного кода в openssl_encrypt

Идентификатор уязвимости: CVE-2026-74883
BDU:2026-11900

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: openssl_encrypt: до 1.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://github.com/jahlives/openssl_encrypt/security/advisories/GHSA-mcjj-qw7m-j3cp
- https://bdu.fstec.ru/vul/2026-11900

11

Краткое описание: Выполнение произвольного кода в GeoServer

Идентификатор уязвимости: BDU:2026-11902

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: GeoServer: от 2.25.3 до 2.28.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://github.com/YonLiud/geoserver-0day-rce/blob/main/README.md
- https://geoserver.org/announcements/vulnerability/2026/08/14/geoserver-2-28-5-released.html
- https://www.securitylab.ru/news/576137.php
- https://sploitus.com/exploit?id=A4039CC7-2E50-5B4C-906C-53025202BDD9
- https://bdu.fstec.ru/vul/2026-11902

Краткое описание: Отказ в обслуживании в Content Credentials JS SDK

Идентификатор уязвимости: CVE-2026-48438
BDU:2026-11917

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Content Credentials JS SDK: до 0.12.1
Content Credentials Rust SDK: до 0.90.6
C2PA Tool: до 0.27.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

12 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://helpx.adobe.com/security/products/content-authenticity-sdk/apsb26-111.html
- https://bdu.fstec.ru/vul/2026-11917

Краткое описание: Отказ в обслуживании в Content Credentials JS SDK

Идентификатор уязвимости: CVE-2026-48439
BDU:2026-11918

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Content Credentials JS SDK: до 0.12.1
Content Credentials Rust SDK: до 0.90.6
C2PA Tool: до 0.27.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

13 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://helpx.adobe.com/security/products/content-authenticity-sdk/apsb26-111.html
- https://bdu.fstec.ru/vul/2026-11918

14

Краткое описание: Получение конфиденциальной информации в Joomla Phoca Cart

Идентификатор уязвимости: CVE-2026-74251
BDU:2026-11901

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Phoca Cart: 3.5.8

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.phoca.cz/news/1506-phoca-cart-version-6-1-7-released-security-release
- https://mysites.guru/blog/phoca-cart-sql-injection-product-filter/
- https://securityvulnerability.io/vulnerability/CVE-2026-74251
- https://bdu.fstec.ru/vul/2026-11901

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-18408
BDU:2026-11972

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

15 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-18408
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11972

16

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-19385
BDU:2026-11973

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-19385
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11973

17

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-6464
BDU:2026-11974

Идентификатор программной ошибки: CWE-829 Использование функций недоверенных источников

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-6464/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11974

18

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-16239
BDU:2026-11969

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-16239
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11969

19

Краткое описание: Отказ в обслуживании в Expat

Идентификатор уязвимости: CVE-2026-66046
BDU:2026-11979

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Expat: до 2.8.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://github.com/libexpat/libexpat/pull/1321
- https://www.vulncheck.com/advisories/expat-denial-of-service-via-storeatts-quadratic-complexity
- https://bdu.fstec.ru/vul/2026-11979

20

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-16238
BDU:2026-11968

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: PostgreSQL: до 18.5
АЛЬТ СП 10: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-16238
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11968

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14676
BDU:2026-11960

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 18.5
АЛЬТ СП 10: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14676
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11960

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-15741
BDU:2026-11966

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-15741
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11966

23

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14662
BDU:2026-11951

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14662
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11951

24

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-15742
BDU:2026-11967

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-15742
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11967

25

Краткое описание: Получение конфиденциальной информации в PostgreSQL

Идентификатор уязвимости: CVE-2026-14668
BDU:2026-11955

Идентификатор программной ошибки: CWE-613 Некорректно настроенный срок действия сессий

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14668
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11955

26

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14670
BDU:2026-11956

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14670
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11956

27

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14664
BDU:2026-11953

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14664
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11953

28

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14677
BDU:2026-11961

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14677
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11961

29

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14679
BDU:2026-11963

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14679
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11963

30

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14680
BDU:2026-11964

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14680
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11964

31

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2026-14671
BDU:2026-11957

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: PostgreSQL: до 14.24
АЛЬТ СП 10: -
Platform V Pangolin DB: 7.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-17 / 2026-08-17

Ссылки на источник:

- https://www.postgresql.org/support/security/CVE-2026-14671
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-11957

32

Краткое описание: Получение конфиденциальной информации в Gitea

Идентификатор уязвимости: CVE-2026-24451
BDU:2026-12010

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.26.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://blog.gitea.com/release-of-1.26.3-and-1.26.4
- https://blog.gitea.com/release-of-1.26.3-and-1.26.4/
- https://github.com/advisories/GHSA-wrf9-r3h7-7x5v
- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/pull/38151
- https://github.com/go-gitea/gitea/releases/tag/v1.26.3
- https://github.com/go-gitea/gitea/security/advisories/GHSA-wrf9-r3h7-7x5v
- https://nvd.nist.gov/vuln/detail/CVE-2026-24451
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12010

33

Краткое описание: Получение конфиденциальной информации в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-42535
BDU:2026-12018

Идентификатор программной ошибки: CWE-668 Возможность несанкционированного доступа к ресурсу

Уязвимый продукт: HTTP Server: до 2.4.68
РЕД ОС: 8.0
Astra Linux Special Edition: 1.7
АЛЬТ СП 10: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/06/08/8
- https://github.com/advisories/GHSA-644r-w2gh-w38h
- https://HTTP Server.apache.org/security/vulnerabilities_24.html
- https://nvd.nist.gov/vuln/detail/CVE-2026-42535
- https://redos.red-soft.ru/support/secure/
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0820SE17
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12018

Краткое описание: Повышение привилегий в ASP.NET Core

Идентификатор уязвимости: CVE-2026-47303
BDU:2026-12015

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
.NET: от 10.0 до 10.0.10
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft Visual Studio 2026: от 18.7 до 18.7.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

34 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47303
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12015

35

Краткое описание: Обход безопасности в ASP.NET Core

Идентификатор уязвимости: CVE-2026-47300
BDU:2026-12014

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: РЕД ОС: 8.0
.NET: от 10.0 до 10.0.10
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft Visual Studio 2026: от 18.7 до 18.7.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47300
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-12014

36

Краткое описание: Повышение привилегий в CoreDNS

Идентификатор уязвимости: CVE-2026-26018
BDU:2026-12012

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: РЕД ОС: 8.0
coredns: до 1.14.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:25127
- https://access.redhat.com/errata/RHSA-2026:36873
- https://access.redhat.com/errata/RHSA-2026:8151
- https://access.redhat.com/security/cve/CVE-2026-26018
- https://bugzilla.redhat.com/show_bug.cgi?id=2445242
- https://github.com/advisories/GHSA-h75p-j8xm-m278
- https://github.com/coredns/coredns
- https://github.com/coredns/coredns/releases/tag/v1.14.2
- https://github.com/coredns/coredns/security/advisories/GHSA-h75p-j8xm-m278
- https://nvd.nist.gov/vuln/detail/CVE-2026-26018

- https://redos.red-soft.ru/support/secure/
- https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-26018.json
- https://bdu.fstec.ru/vul/2026-12012

37

Краткое описание: Получение конфиденциальной информации в phpMyFAQ

Идентификатор уязвимости: CVE-2026-75918
BDU:2026-12006

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: phpMyFAQ: до 4.1.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-j5w2-cwwj-xj7x
- https://bdu.fstec.ru/vul/2026-12006

38

Краткое описание: Чтение локальных файлов в MLflow

Идентификатор уязвимости: CVE-2026-64849
BDU:2026-12002

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: MLflow: до 3.13.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.3 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://github.com/mlflow/mlflow/security/advisories/GHSA-7gwp-5pfp-969j
- https://thehackernews.com/2026/08/attackers-exploit-mlflow-ssrf-flaw-to.html
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-64849
- https://www.securityweek.com/mlflow-vulnerability-exploited-for-cloud-credential-theft/
- https://github.com/mlflow/mlflow/releases/tag/v3.15.0
- https://github.com/mlflow/mlflow/issues/24179
- https://github.com/BiuTrap/CVE-2026-64849
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-12002

39

Краткое описание: Выполнение произвольного кода в Metabase

Идентификатор уязвимости: CVE-2026-72898
BDU:2026-12003

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Metabase: до 0.63.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://www.metabase.com/blog/security-update-6-aug-2026
- https://horizon3.ai/attack-research/vulnerabilities/cve-2026-72898/
- https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-72898
- https://github.com/codeb0ssx/CVE-2026-72898-PoC
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-12003

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46326
BDU:2026-12217

Идентификатор программной ошибки: CWE-909 Отсутствует инициализация ресурса

Уязвимый продукт: Linux: от 6.9 до 6.12.75
Astra Linux Special Edition: 4.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

40

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46326
- https://security-tracker.debian.org/tracker/CVE-2026-46326
- https://git.kernel.org/linus/1e0ac56c92e26115cbc8cfc639843725cb3a7d6a
- https://git.kernel.org/stable/c/1e0ac56c92e26115cbc8cfc639843725cb3a7d6a
- https://git.kernel.org/stable/c/664ffdf34c01810085e4d85508b361c3fdd2ab40
- https://git.kernel.org/stable/c/72158f9ae29a9e56d0f9704ce461a866feaf9925
- https://git.kernel.org/stable/c/9080c7ac30f5f8f8fcb7b27b56df60fea7909c21
- https://github.com/torvalds/linux/commit/9080c7ac30f5f8f8fcb7b27b56df60fea7909c21
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18
- https://bdu.fstec.ru/vul/2026-12217

41

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45938
BDU:2026-12207

Идентификатор программной ошибки: CWE-364 Состояние гонки, связанное с обработчиком сигналов

Уязвимый продукт: Linux: от 6.7 до 6.12.75
Astra Linux Special Edition: 4.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45938
- https://security-tracker.debian.org/tracker/CVE-2026-45938
- https://git.kernel.org/linus/b7508129978ae1e2ed9b0410396abc05def9c4eb
- https://git.kernel.org/stable/c/08e674e9862a2db46fb234eb7c5442455ece0131
- https://git.kernel.org/stable/c/b7508129978ae1e2ed9b0410396abc05def9c4eb
- https://git.kernel.org/stable/c/d7d31fc99d248d5f47588f50dce5c7599c991c6a
- https://git.kernel.org/stable/c/dbe579e620ef0f53db490ec79a8566e4ea8918ac
- https://github.com/torvalds/linux/commit/d7d31fc99d248d5f47588f50dce5c7599c991c6a
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18
- https://bdu.fstec.ru/vul/2026-12207

42

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45898
BDU:2026-12198

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 6.11 до 6.12.75
Astra Linux Special Edition: 4.8

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45898
- https://security-tracker.debian.org/tracker/CVE-2026-45898
- https://git.kernel.org/linus/7874eeacfa42177565c01d5198726671acf7adf2
- https://git.kernel.org/stable/c/38c5b49fffa1b760959af74f11806eeb3ef4706d
- https://git.kernel.org/stable/c/7874eeacfa42177565c01d5198726671acf7adf2
- https://git.kernel.org/stable/c/a6b9e793e74e372daa266fd0d58b751305877897
- https://git.kernel.org/stable/c/eb715133e0ae12514bba4d2d5ce1dee774476056
- https://github.com/torvalds/linux/commit/a6b9e793e74e372daa266fd0d58b751305877897
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18
- https://bdu.fstec.ru/vul/2026-12198

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31717
BDU:2026-12170

Идентификатор программной ошибки: CWE-708 Некорректное назначение владельца

Уязвимый продукт: Linux: от 6.9 до 6.18.25
Astra Linux Special Edition: 4.8
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

43

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-31717
- https://security-tracker.debian.org/tracker/CVE-2026-31717
- https://git.kernel.org/linus/49110a8ce654bbe56bef7c5e44cce31f4b102b8a
- https://git.kernel.org/stable/c/00ce8d6789dae72d042a4522264964c72891ca37
- https://git.kernel.org/stable/c/49110a8ce654bbe56bef7c5e44cce31f4b102b8a
- https://git.kernel.org/stable/c/c908c853f304a4969b5aa10eba0b50350cc65b80
- https://github.com/TurtleARM/CVE-2026-31717-KSMBD-Exploit
- https://lore.kernel.org/linux-cve-announce/2026050124-CVE-2026-31717-f68b@gregkh/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0626SE18
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12170

44

Краткое описание: Повышение привилегий в Wazuh

Идентификатор уязвимости: CVE-2026-44252
BDU:2026-12057

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Wazuh: от 4.0.0 до 4.14.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-34fx-c2xw-xcpg
- https://github.com/wazuh/wazuh/pull/35307
- http://github.com/wazuh/wazuh/releases/tag/v4.14.5
- https://github.com/wazuh/wazuh/commit/b3459f5663702aea14e91330a7a6912081fed2eb
- https://bdu.fstec.ru/vul/2026-12057

45

Краткое описание: Выполнение произвольного кода в Wazuh

Идентификатор уязвимости: CVE-2026-49441
BDU:2026-12056

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: Wazuh: от 4.3.0 до 4.14.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-3v57-hgvj-3vj2
- https://github.com/wazuh/wazuh/commit/7f13682cf5f01f69452f723a608ab2d89cfb2133
- http://github.com/wazuh/wazuh/releases/tag/v4.14.6
- https://github.com/wazuh/wazuh/pull/36296
- https://bdu.fstec.ru/vul/2026-12056

46

Краткое описание: Выполнение произвольного кода в Wazuh

Идентификатор уязвимости: CVE-2026-48024
BDU:2026-12055

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Wazuh: от 4.0.0 до 4.14.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-gh4h-fx78-q8xc
- https://github.com/wazuh/wazuh/commit/88fc89fdfb1bf37b9d826e9c281a3d22655733de
- https://github.com/wazuh/wazuh/pull/36204
- https://github.com/wazuh/wazuh/releases/tag/v4.14.6
- https://bdu.fstec.ru/vul/2026-12055

47

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-76928
BDU:2026-12054

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.18

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-87.html
- https://gitlab.com/wireshark/wireshark/-/work_items/21469
- https://bdu.fstec.ru/vul/2026-12054

Краткое описание: Внедрение кода в phpMyFAQ

Идентификатор уязвимости: CVE-2026-76208
BDU:2026-12052

Идентификатор программной ошибки: CWE-778 Некорректное журналирование

Уязвимый продукт: phpMyFAQ: до 4.1.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Внедрение кода

48 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-8pr3-q3cw-q234
- https://bdu.fstec.ru/vul/2026-12052

Краткое описание: Получение конфиденциальной информации в phpMyFAQ

Идентификатор уязвимости: CVE-2026-76207
BDU:2026-12051

Идентификатор программной ошибки: CWE-304 Пропущен важный шаг аутентификации

Уязвимый продукт: phpMyFAQ: до 4.1.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

49 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-hvj7-4fmg-53cr
- https://bdu.fstec.ru/vul/2026-12051

50

Краткое описание: Получение конфиденциальной информации в phpMyFAQ

Идентификатор уязвимости: CVE-2026-76205
BDU:2026-12050

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: phpMyFAQ: до 4.1.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-79h3-6hxj-g98h
- https://bdu.fstec.ru/vul/2026-12050

51

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-76879
BDU:2026-12049

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.18

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-89.html
- https://gitlab.com/wireshark/wireshark/-/work_items/21480
- https://bdu.fstec.ru/vul/2026-12049

52

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-76886
BDU:2026-12046

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.18

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-75.html
- https://gitlab.com/wireshark/wireshark/-/work_items/21446
- https://gitlab.com/wireshark/wireshark/-/work_items/21439
- https://bdu.fstec.ru/vul/2026-12046

53

Краткое описание: Выполнение произвольного кода в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-69836
BDU:2026-12045

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft Entra ID: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69836
- https://thehackernews.com/2026/08/microsoft-entra-id-flaw-cvss-100.html
- https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-max-severity-entra-id-flaw-exploited-in-attacks/
- https://thecyberexpress.com/microsoft-entra-id-cve-2026-69836-exploited/
- https://bdu.fstec.ru/vul/2026-12045

Краткое описание: Получение конфиденциальной информации в Unbound

Идентификатор уязвимости: CVE-2026-40622
BDU:2026-12030

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: РЕД ОС: 8.0
Unbound: от 1.16.2 до 1.25.0 включительно
АЛЬТ СП 10: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

54

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.nlnetlabs.nl/downloads/unbound/CVE-2026-40622.txt
- https://redos.red-soft.ru/support/secure/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12030

55

Краткое описание: Получение конфиденциальной информации в CoreDNS

Идентификатор уязвимости: CVE-2026-33489
BDU:2026-12027

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
coredns: до 1.14.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://github.com/advisories/GHSA-h8mm-c463-wjq3
- https://github.com/coredns/coredns
- https://github.com/coredns/coredns/releases/tag/v1.14.3
- https://github.com/coredns/coredns/security/advisories/GHSA-h8mm-c463-wjq3
- https://nvd.nist.gov/vuln/detail/CVE-2026-33489
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12027

56

Краткое описание: Обход безопасности в CoreDNS

Идентификатор уязвимости: CVE-2026-33190
BDU:2026-12026

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: РЕД ОС: 8.0
coredns: до 1.14.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://github.com/advisories/GHSA-qhmp-q7xh-99rh
- https://github.com/coredns/coredns
- https://github.com/coredns/coredns/releases/tag/v1.14.3
- https://github.com/coredns/coredns/security/advisories/GHSA-qhmp-q7xh-99rh
- https://nvd.nist.gov/vuln/detail/CVE-2026-33190
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12026

57

Краткое описание: Отказ в обслуживании в CoreDNS

Идентификатор уязвимости: CVE-2026-32936
BDU:2026-12025

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: РЕД ОС: 8.0
coredns: до 1.14.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://github.com/advisories/GHSA-63cw-r7xf-jmwr
- https://github.com/coredns/coredns
- https://github.com/coredns/coredns/releases/tag/v1.14.3
- https://github.com/coredns/coredns/security/advisories/GHSA-63cw-r7xf-jmwr
- https://nvd.nist.gov/vuln/detail/CVE-2026-32936
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12025

Краткое описание: Отказ в обслуживании в CoreDNS

Идентификатор уязвимости: CVE-2026-32934
BDU:2026-12024

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: РЕД ОС: 8.0
coredns: до 1.14.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

58 **Оценка CVSSv3:** 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://github.com/advisories/GHSA-2wpx-qpw2-g5h5
- https://github.com/coredns/coredns
- https://github.com/coredns/coredns/releases/tag/v1.14.3
- https://github.com/coredns/coredns/security/advisories/GHSA-2wpx-qpw2-g5h5
- https://github.com/coredns/coredns/security/advisories/GHSA-cvx7-x8pj-x2gw
- https://nvd.nist.gov/vuln/detail/CVE-2026-32934
- https://redos.red-soft.ru/support/secure/
- https://bdu.fstec.ru/vul/2026-12024

Краткое описание: Выполнение произвольного кода в Libheif

Идентификатор уязвимости: CVE-2026-32740
BDU:2026-12022

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: РЕД ОС: 8.0
Libheif: до 1.22.0
АЛЬТ СП 10: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

59

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-32740
- https://bugzilla.redhat.com/show_bug.cgi?id=2479969
- https://github.com/strukturag/libheif/releases/tag/v1.22.0
- https://github.com/strukturag/libheif/security/advisories/GHSA-frfr-f3vg-2g6j
- https://nvd.nist.gov/vuln/detail/CVE-2026-32740
- https://redos.red-soft.ru/support/secure/
- https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-32740.json
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12022

60

Краткое описание: Перезапись произвольных файлов в GitPython

Идентификатор уязвимости: CVE-2026-76219
BDU:2026-12059

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: GitPython: до 3.1.58

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Перезапись произвольных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-4gmw-gg2m-w46p
- https://bdu.fstec.ru/vul/2026-12059

61

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-76220
BDU:2026-12060

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: GitPython: до 3.1.58

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-wvpp-8hx9-p66j
- https://bdu.fstec.ru/vul/2026-12060

62

Краткое описание: Перезапись произвольных файлов в GitPython

Идентификатор уязвимости: CVE-2026-76222
BDU:2026-12062

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: GitPython: до 3.1.58

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Перезапись произвольных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-hmq2-w58f-27jc
- https://bdu.fstec.ru/vul/2026-12062

63

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-76221
BDU:2026-12061

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: GitPython: до 3.1.58

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-jm78-9fvv-mhgr
- https://bdu.fstec.ru/vul/2026-12061

64

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43125
BDU:2026-12095

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19 до 6.19.5 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43125
- https://git.kernel.org/stable/c/67288113c5e6cf9e659b4065c0ed6f16100e0c71
- https://git.kernel.org/stable/c/082083c9fbd99422a0370fe2102144a231c9f5d6
- https://git.kernel.org/stable/c/5f053a2e7209d326cbbc07738fa6d6893d307438
- https://git.kernel.org/linus/080e5563f878c64e697b89e7439d730d0daad882
- https://lore.kernel.org/linux-cve-announce/2026050619-CVE-2026-43125-c9f9@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43125
- https://access.redhat.com/security/cve/cve-2026-43125

- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12095

65

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43383
BDU:2026-12091

Идентификатор программной ошибки: CWE-208 Разглашение информации, связанное с временной разницей при выполнении операций

Уязвимый продукт: Linux: от 5.11 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43383
- https://git.kernel.org/stable/c/821c8751fdeecdeecabeb11704dd33439c9e4bbc
- https://git.kernel.org/stable/c/345a9530756528d7ca407663d659c3c40e75c3dd
- https://git.kernel.org/stable/c/5d305a95130a8d08b9545e47f1e18d29d59866cb
- https://git.kernel.org/stable/c/02669e2a4d207068edce7e8b5fafd85822018ce6
- https://git.kernel.org/stable/c/ae3831b44f477de048287493e184fc3ff913b624

- https://git.kernel.org/stable/c/b502e97e29d791ff7a8051f29a414535739be218
- https://git.kernel.org/linus/46d0d6f50dab706637f4c18a470aac20a21900d3
- https://lore.kernel.org/linux-cve-announce/2026050833-CVE-2026-43383-0333@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43383
- https://access.redhat.com/security/cve/cve-2026-43383
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12091

66

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43198
BDU:2026-12089

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 2.6.12 до 6.18.15 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43198
- https://git.kernel.org/stable/c/fe89b2f05b85847784f91127319172945c1fadd
- https://git.kernel.org/stable/c/7178e2a8027423b2af17ab95df73a749a5b72e5b
- https://git.kernel.org/linus/858d2a4f67ff69e645a43487ef7ea7f28f06deae
- https://lore.kernel.org/linux-cve-announce/2026050645-CVE-2026-43198-0870@gregkh/
- https://access.redhat.com/security/cve/cve-2026-43198
- https://bdu.fstec.ru/vul/2026-12089

67

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43407
BDU:2026-12084

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Linux: от 2.6.34 до 5.10.252 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43407
- https://git.kernel.org/stable/c/ea080b21092590122c3f971cf588932cdbf47847
- https://git.kernel.org/stable/c/edc678e5cd11730a2834b43071d8923f05bc334d
- https://git.kernel.org/stable/c/6cee34d6669fe176b4259131adb1a145c939b472
- https://git.kernel.org/stable/c/8bb87547e92dcf0928ed763c60e0ac8d733c3656
- https://git.kernel.org/stable/c/ed024d2f4c79c0eb2464df0fb640610ac301f9a0
- https://git.kernel.org/stable/c/f9da5c1bbac5c8e33259fe00ed7347438fffa969

- https://git.kernel.org/stable/c/9f9e2297f45fc2d2524eb104c289d69ddef95665
- https://git.kernel.org/linus/b282c43ed156ae15ea76748fc15cd5c39dc9ab72
- https://lore.kernel.org/linux-cve-announce/2026050842-CVE-2026-43407-d1e9@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43407
- https://access.redhat.com/security/cve/CVE-2026-43407
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12084

68

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43117
BDU:2026-12086

Идентификатор программной ошибки: CWE-404 Некорректное освобождение ресурсов

Уязвимый продукт: Linux: от 6.7 до 6.12.82 включительно
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43117
- https://git.kernel.org/stable/c/c09a7446aab5773f38d6abb25fce99b8e1dfbc97
- https://git.kernel.org/stable/c/32372781d664a9b03c40343e96c29d0a6139f97d
- https://git.kernel.org/stable/c/2e4adfaec97ee053ad1bdfb5036845e66f7e0d8a
- https://git.kernel.org/stable/c/d110d7cdb045715c0b45b0dfd974525bb38f653d
- https://git.kernel.org/linus/a85b46db143fda5869e7d8df8f258ccef5fa1719
- https://lore.kernel.org/linux-cve-announce/2026050627-CVE-2026-43117-8e20@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43117

- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12086

69

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43197
BDU:2026-12087

Идентификатор программной ошибки: CWE-170 Некорректное использование нулевых символов

Уязвимый продукт: Linux: от 6.6 до 6.18.15 включительно
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43197
- https://git.kernel.org/stable/c/3126a2f98beaec5a554a1fb31c46db1e8542665e
- https://git.kernel.org/stable/c/74ab1456eaa3b2eb986138f9e1f4cb37e73b6f58
- https://git.kernel.org/linus/82aec772fca2223bc5774bd9af486fd95766e578
- https://lore.kernel.org/linux-cve-announce/2026050644-CVE-2026-43197-37f5@gregkh/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12087

70

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43406
BDU:2026-12088

Идентификатор программной ошибки: CWE-805 Доступ к памяти за пределами буфера

Уязвимый продукт: Linux: от 5.16 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://git.kernel.org/linus/69fb5d91bba44ecf7eb80530b85fa4fb028921d5
- https://www.cve.org/CVERecord?id=CVE-2026-43406
- https://git.kernel.org/stable/c/76ccf21a12c5f6d6790bc32c7da82446d877b2f4
- https://git.kernel.org/stable/c/75582aaa580c11aed4c7731cad6b068b700e7efb
- https://git.kernel.org/stable/c/50156622eb0888e62541d715a98584480a1bc7cb
- https://git.kernel.org/stable/c/dbd857a9e1e33ea71eaf3e211877027e533770d1
- https://git.kernel.org/stable/c/69fe5af33fa3806f398d21c081d73c66e5523bc2
- https://git.kernel.org/stable/c/035867ae6f18df0aeedb2a57a5b74091bd4e3fe8

- https://lore.kernel.org/linux-cve-announce/2026050842-CVE-2026-43406-84a2@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43406
- https://access.redhat.com/security/cve/cve-2026-43406
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12088

71

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43083
BDU:2026-12085

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 5.17 до 6.18.23 включительно
Red Hat Enterprise Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43083
- https://git.kernel.org/stable/c/6d1d9ed9b409e0662241e3d245d574a18f643494
- https://git.kernel.org/stable/c/95a1334748c95dd15546056280ade0c4b8dd7b78
- https://git.kernel.org/linus/b30b1675aa2bcf0491fd3830b051df4e08a7c8ca
- https://lore.kernel.org/linux-cve-announce/2026050615-CVE-2026-43083-c69b@gregkh/
- https://access.redhat.com/security/cve/cve-2026-43083
- https://bdu.fstec.ru/vul/2026-12085

72

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31476
BDU:2026-12527

Идентификатор программной ошибки: CWE-404 Некорректное освобождение ресурсов

Уязвимый продукт: Linux: от 5.15 до 6.1.167 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/e0e5edc81b241c70355217de7e120c97c3429deb
- https://git.kernel.org/stable/c/6fafc4c4238e538969f1375f9ecdc6587c53f1cc
- https://git.kernel.org/stable/c/f5300690c23c5ac860499bb37dbc09cf43fd62e6
- https://git.kernel.org/stable/c/1d1888b4a7aec518b707f6eca0bf08992c0e8da3
- https://git.kernel.org/stable/c/a897064a457056acb976e20e3007cdf553de340f
- https://www.cve.org/CVERecord?id=CVE-2026-31476
- https://git.kernel.org/linus/9bbb19d21ded7d78645506f20d8c44895e3d0fb9
- https://security-tracker.debian.org/tracker/CVE-2026-31476

- https://ubuntu.com/security/CVE-2026-31476
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12527

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31501
BDU:2026-12537

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.15 до 6.19.10 включительно
Ubuntu: 24.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

73

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/d5827316debcb677679bb014885d7be92c410e11
- https://www.cve.org/CVERecord?id=CVE-2026-31501
- https://git.kernel.org/linus/eb8c426c9803beb171f89d15fea17505eb517714
- https://ubuntu.com/security/CVE-2026-31501
- https://bdu.fstec.ru/vul/2026-12537

74

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31513
BDU:2026-12544

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19.6 до 6.19.10 включительно
Red Hat Enterprise Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/5b35f8211a913cfe7ab9d54fa36a272d2059a588
- https://git.kernel.org/stable/c/a3d9c50d69785ae02e153f000da1b5fd6dbfdf1b
- https://git.kernel.org/stable/c/c8e1a27edb8b4e5afb56b384acd7b6c2dec1b7cc
- https://www.cve.org/CVERecord?id=CVE-2026-31513
- https://git.kernel.org/linus/9d87cb22195b2c67405f5485d525190747ad5493
- https://access.redhat.com/security/cve/CVE-2026-31513
- https://bdu.fstec.ru/vul/2026-12544

75

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31396
BDU:2026-12505

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.11 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31396
- https://git.kernel.org/stable/c/341d01087f821aa0f165fb1ffc8bfe4e50776da7
- https://git.kernel.org/stable/c/5653af416a48f6c18f9626ae9df96f814f45ff34
- https://git.kernel.org/stable/c/0bb848d8c64938024e45780f8032f1f67d3a3607
- https://git.kernel.org/stable/c/1f4714065b2bcbb0a4013fd355b84b848e6cc345
- https://git.kernel.org/stable/c/eb652535e9ec795ef5c1078f7578eaaed755268b
- https://git.kernel.org/linus/8da13e6d63c1a97f7302d342c89c4a56a55c7015

- https://security-tracker.debian.org/tracker/CVE-2026-31396
- https://ubuntu.com/security/CVE-2026-31396
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12505

76

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23424
BDU:2026-12486

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.14 до 6.18.16 включительно
Ubuntu: 24.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://git.kernel.org/linus/901ec3470994006bc8dd02399e16b675566c3416
- https://www.cve.org/CVERecord?id=CVE-2026-23424
- https://git.kernel.org/stable/c/3464e751755172ddbb849c1bd92f5f59e95c59a1
- https://git.kernel.org/stable/c/3ed2ae6b3fe869f99b75afd02045ba5c0c0773e2
- https://ubuntu.com/security/CVE-2026-23424
- https://bdu.fstec.ru/vul/2026-12486

77

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31536
BDU:2026-12553

Идентификатор программной ошибки: CWE-166 Некорректная обработка отсутствующих специальных элементов

Уязвимый продукт: Linux: от 5.15 до 6.18.10 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/e38b415c024bc3b6321bf8650dbf3f4aab8e74b3
- https://git.kernel.org/stable/c/24082642654f3e5149913946e89c00a297a8868f
- https://www.cve.org/CVERecord?id=CVE-2026-31536
- https://git.kernel.org/linus/9da82dc73cb03e85d716a2609364572367a5ff47
- https://bdu.fstec.ru/vul/2026-12553

78

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23427
BDU:2026-12488

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 6.19.9 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://git.kernel.org/linus/b425e4d0eb321a1116ddbf39636333181675d8f4
- https://www.cve.org/CVERecord?id=CVE-2026-23427
- https://git.kernel.org/stable/c/b0158d9d6f4ec5941e49a0b812735db2844f9975
- https://git.kernel.org/stable/c/568a25fd7bcdfb2790f7d42aa2a440dca4435c96
- https://git.kernel.org/stable/c/a5828c14a9e3d5eeed0bcc0a58f0f3fbca0cdcb2
- https://git.kernel.org/stable/c/9b0792c3eacf01e67f356d6ef9707b0ae5022419
- https://security-tracker.debian.org/tracker/CVE-2026-23427
- https://ubuntu.com/security/CVE-2026-23427

- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12488

79

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23428
BDU:2026-12489

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.3.10 до 6.6.129 включительно
Ubuntu: 25.10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://git.kernel.org/linus/c33615f995aee80657b9fdfbc4ee7f49c2bd733d
- https://www.cve.org/CVERecord?id=CVE-2026-23428
- https://git.kernel.org/stable/c/eae0dc86f71e6f3294c0cd7ffc05039258d243af
- https://git.kernel.org/stable/c/806f13752652216db0c309392b4db3e64eeed4f2
- https://git.kernel.org/stable/c/c742b46a153d3ff95ff0825ab1950c87b9e14470
- https://git.kernel.org/stable/c/7f7468fd2a7554cea91b7d430335a3dbf01dcc09
- https://git.kernel.org/stable/c/a5929c2020ce54e1dcbd1078c0f30b8aaf73c105
- https://security-tracker.debian.org/tracker/CVE-2026-23428

- https://ubuntu.com/security/CVE-2026-23428
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12489

80

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23432
BDU:2026-12492

Идентификатор программной ошибки: CWE-763 Освобождение недопустимого указателя или ссылки

Уязвимый продукт: Linux: от 6.19 до 6.19.9 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://git.kernel.org/linus/6922db250422a0dfee34de322f86b7a73d713d33
- https://www.cve.org/CVERecord?id=CVE-2026-23432
- https://git.kernel.org/stable/c/34861bdc0c0196b6c2dd48f7454029407704ff6e
- https://bdu.fstec.ru/vul/2026-12492

81

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23446
BDU:2026-12495

Идентификатор программной ошибки: CWE-833 Взаимоблокировка

Уязвимый продукт: Linux: от 5.0 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23446
- https://git.kernel.org/stable/c/621f2f43741b51f62d767eb4752fbcefe2526926
- https://git.kernel.org/stable/c/4de6a43e8ecf961feabddf0e9d6911081d2ed218
- https://git.kernel.org/stable/c/3267bcb744ee8a2feabaa7ab69473f086f67fd71
- https://git.kernel.org/stable/c/d3e32a612c6391ca9b7c183aeec22b4fd24c300c
- https://git.kernel.org/stable/c/98e8aed64614b0c199d5f0391fbe1a4331cb5773
- https://git.kernel.org/linus/069c8f5aebe4d5224cf62acc7d4b3486091c658a

- https://security-tracker.debian.org/tracker/CVE-2026-23446
- https://ubuntu.com/security/CVE-2026-23446
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12495

82

Краткое описание: Перезапись произвольных файлов в Linux

Идентификатор уязвимости: CVE-2026-23459
BDU:2026-12497

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.14 до 6.19.9 включительно
Ubuntu: 24.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Перезапись произвольных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23459
- https://git.kernel.org/stable/c/0d087d00161f562d5047cc4009bb0c6a19daf9f1
- https://git.kernel.org/linus/8431c602f551549f082bbfa67f3003f2d8e3e132
- https://ubuntu.com/security/CVE-2026-23459
- https://bdu.fstec.ru/vul/2026-12497

83

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31405
BDU:2026-12506

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 2.6.12 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31405
- https://git.kernel.org/stable/c/29ef43ceb121d67b87f4cbb08439e4e9e732eff8
- https://git.kernel.org/stable/c/1a6da3dbb9985d00743073a1cc1f96e59f5abc30
- https://git.kernel.org/stable/c/145e50c2c700fa52b840df7bab206043997dd18e
- https://git.kernel.org/stable/c/8bde543d2a5f935ba2a6a6325a2e02f8a9256fbe
- https://git.kernel.org/stable/c/f2b65dcb78c8990e4c68a906627433be1fe38a92
- https://git.kernel.org/linus/24d87712727a5017ad142d63940589a36cd25647

- https://security-tracker.debian.org/tracker/CVE-2026-31405
- https://ubuntu.com/security/CVE-2026-31405
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12506

84

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31412
BDU:2026-12507

Идентификатор программной ошибки: CWE-1073 Вызываемый не-SQL элемент управления с большим количеством обращений к данным

Уязвимый продукт: Linux: от 3.3 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31412
- https://git.kernel.org/stable/c/91817ad5452defe69bc7bc0e355f0ed5d01125cc
- https://git.kernel.org/stable/c/ce0caaed5940162780c5c223b8ae54968a5f059b
- https://git.kernel.org/stable/c/228b37936376143f4b60cc6828663f6eaceb81b5
- https://git.kernel.org/stable/c/3428dc5520c811e66622b2f5fa43341bf9a1f8b3
- https://git.kernel.org/stable/c/387ebb0453b99d71491419a5dc4ab4bee0cacbac
- https://git.kernel.org/linus/8479891d1f04a8ce55366fe4ca361ccdb96f02e1

- https://security-tracker.debian.org/tracker/CVE-2026-31412
- https://ubuntu.com/security/CVE-2026-31412
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12507

85

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31417
BDU:2026-12508

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Linux: от 6.19 до 6.19.11 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31417
- https://git.kernel.org/stable/c/6e568835ea54a3e1d08e310e34f95d434e739477
- https://git.kernel.org/stable/c/1734bd85c5e0a7a801295b729efb56b009cb8fc3
- https://git.kernel.org/stable/c/4e2d1bcef78d21247fe8fef13bc7ed95885df2b5
- https://git.kernel.org/stable/c/8c92969c197b91c134be27dc3afb64ab468853a9
- https://git.kernel.org/stable/c/f953f11ccf4afe6feb635c08145f4240d9a6b544
- https://git.kernel.org/linus/a1822cb524e89b4cd2cf0b82e484a2335496a6d9

- https://security-tracker.debian.org/tracker/CVE-2026-31417
- https://ubuntu.com/security/CVE-2026-31417
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12508

86

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31433
BDU:2026-12511

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.6 до 6.6.130 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31433
- https://git.kernel.org/stable/c/3a852f9d1c981fb14f6bf4e24999e0ea8088a7d7
- https://git.kernel.org/stable/c/4cca3eff2099b18672934a39cee70aed835d652c
- https://git.kernel.org/stable/c/358cdaa1f7fbf2712cb4c5f6b59cb9a5c673c5fe
- https://git.kernel.org/stable/c/7aec5a769d2356cbf344d85bcfd36de592ac96a5
- https://git.kernel.org/stable/c/b0cd9725fe2bcc9f37d096b132318a9060373f5d
- https://git.kernel.org/stable/c/9d7032851d6f5adbe2739601ca456c0ad3b422f0
- https://git.kernel.org/linus/beef2634f81f1c086208191f7228bce1d366493d

- https://security-tracker.debian.org/tracker/CVE-2026-31433
- https://ubuntu.com/security/CVE-2026-31433
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12511

87

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31463
BDU:2026-12522

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: Linux: от 6.19 до 6.19.10 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31463
- https://git.kernel.org/stable/c/4a927f670cdb0def226f9f85f42a9f19d9e09c88
- https://git.kernel.org/linus/bd71fb3fea9945987053968f028a948997cba8cc
- https://bdu.fstec.ru/vul/2026-12522

88

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31553
BDU:2026-12559

Идентификатор программной ошибки: CWE-468 Некорректное масштабирование указателей

Уязвимый продукт: Linux: от 6.19 до 6.19.10 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/4307e05e568782fc92eff651b09ee5dee88a058d
- https://www.cve.org/CVERecord?id=CVE-2026-31553
- https://git.kernel.org/linus/0496acc42fb51eee040b5170cec05cec41385540
- https://bdu.fstec.ru/vul/2026-12559

89

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31659
BDU:2026-12598

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Linux: от 3.13 до 5.10.252 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/cf2199171ef799ca7270019125f4a91bd20ad4d9
- https://git.kernel.org/stable/c/95c71365a2222908441b54d6f2c315e0c79fcec3
- https://git.kernel.org/stable/c/f970646b9a39539d1bac86822ac78b5915455ea9
- https://git.kernel.org/stable/c/de6c1dc3c7d01a152607e6fcecee4d5288283f10
- https://git.kernel.org/stable/c/7e5d007e0df946bffb8542fb112e0044014a5897
- https://git.kernel.org/stable/c/69d61639bc7e963c3b645e570279d731e7c89062
- https://git.kernel.org/stable/c/2997f4bd1f982e7013709946e00be89b507693fa

- https://www.cve.org/CVERecord?id=CVE-2026-31659
- https://git.kernel.org/linus/3a359bf5c61d52e7f09754108309d637532164a6
- https://security-tracker.debian.org/tracker/CVE-2026-31659
- https://ubuntu.com/security/CVE-2026-31659
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12598

90

Краткое описание: Выполнение произвольного кода в JSONata

Идентификатор уязвимости: CVE-2026-77413
BDU:2026-12626

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: JSONata: до 1.8.7 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://github.com/jsonata-js/jsonata/releases/tag/v1.8.8
- https://github.com/jsonata-js/jsonata/releases/tag/v2.2.0
- https://github.com/jsonata-js/jsonata/pull/794
- https://github.com/jsonata-js/jsonata/security/advisories/GHSA-8gq3-vp5j-2grp
- https://bdu.fstec.ru/vul/2026-12626

91

Краткое описание: Выполнение произвольного кода в JSONata

Идентификатор уязвимости: CVE-2026-77414
BDU:2026-12627

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: JSONata: до 1.8.8

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://github.com/jsonata-js/jsonata/releases/tag/v1.8.8
- https://github.com/jsonata-js/jsonata/releases/tag/v2.2.1
- https://github.com/jsonata-js/jsonata/pull/799
- https://github.com/jsonata-js/jsonata/security/advisories/GHSA-2943-5xfg-gq5f
- https://bdu.fstec.ru/vul/2026-12627

Краткое описание: Выполнение произвольного кода в JSONata

Идентификатор уязвимости: CVE-2026-77415
BDU:2026-12628

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: JSONata: до 1.8.8

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

92

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://github.com/jsonata-js/jsonata/releases/tag/v1.8.8
- https://github.com/jsonata-js/jsonata/releases/tag/v2.2.1
- https://github.com/jsonata-js/jsonata/pull/799
- https://github.com/jsonata-js/jsonata/pull/800
- https://github.com/jsonata-js/jsonata/pull/802
- https://github.com/jsonata-js/jsonata/security/advisories/GHSA-66mm-25pp-rfff
- https://bdu.fstec.ru/vul/2026-12628

93

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31558
BDU:2026-12561

Идентификатор программной ошибки: CWE-839 Отсутствует проверка на соответствие минимальному значению диапазона

Уязвимый продукт: Linux: от 6.10 до 6.12.79 включительно
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/878cf6acb4fd8ab4126cf9d369a5bb0e23123418
- https://git.kernel.org/stable/c/596c3f8069c4792f22fce8c4452f44410032d910
- https://git.kernel.org/stable/c/47857b05bd50db01e211a1b6f513d57901cd3e6b
- https://www.cve.org/CVERecord?id=CVE-2026-31558
- https://git.kernel.org/linus/2db06c15d8c7a0ccb6108524e16cd9163753f354
- https://security-tracker.debian.org/tracker/CVE-2026-31558
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12561

94

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31608
BDU:2026-12584

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 6.19.1 до 6.19.13 включительно
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/2ba03f46132b0d1a7bafb86e1ef61951a2254023
- https://git.kernel.org/stable/c/6968c91fab05b8fc4d6700e0cf34472bb422df25
- https://git.kernel.org/stable/c/830de6eeb9db4cb7e758201fb99328ef4ca4b032
- https://www.cve.org/CVERecord?id=CVE-2026-31608
- https://git.kernel.org/linus/84ff995ae826aa6bbcc6c7b9ea569ff67c021d72
- https://ubuntu.com/security/CVE-2026-31608
- https://bdu.fstec.ru/vul/2026-12584

95

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31611
BDU:2026-12585

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.15 до 6.12.82 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/08f9e6d899b5c834bbcc239eae1bed58d9b15d2c
- https://git.kernel.org/stable/c/9401f86a224f37b50e6a3ccf1d46a70d5ef8af0a
- https://git.kernel.org/stable/c/46bbcd3ebfb3549c8da1838fc4493e79bd3241e7
- https://git.kernel.org/stable/c/d2454f4a002d08560a60f214f392e6491cf11560
- https://git.kernel.org/stable/c/b5b5d5936a50497fb151c0b122899a6894721c2b
- https://www.cve.org/CVERecord?id=CVE-2026-31611
- https://git.kernel.org/linus/53370cf9090777774e07fd9a8ebce67c6cc333ab
- https://security-tracker.debian.org/tracker/CVE-2026-31611

- https://ubuntu.com/security/CVE-2026-31611
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12585

96

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31613
BDU:2026-12586

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.0.16 до 6.18.23 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://git.kernel.org/stable/c/e0dd90d14cbbf318157ea8e3fb62ee68a28655ed
- https://git.kernel.org/stable/c/781902e069f4ecb6c3b83502f181972c1446110a
- https://git.kernel.org/stable/c/a66ef2e7ed837325c5600f8617d5ee0a0a149fdd
- https://www.cve.org/CVERecord?id=CVE-2026-31613
- https://git.kernel.org/linus/3df690bba28edec865cf7190be10708ad0ddd67e
- https://security-tracker.debian.org/tracker/CVE-2026-31613
- https://access.redhat.com/security/cve/CVE-2026-31613
- https://ubuntu.com/security/CVE-2026-31613

- https://bdu.fstec.ru/vul/2026-12586

97

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23372
BDU:2026-12478

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.1 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23372
- https://git.kernel.org/stable/c/3ae592ed91bb4b6b51df256b51045c13d2656049
- https://git.kernel.org/stable/c/722a28b635ec281bb08a23885223526d8e7d6526
- https://git.kernel.org/stable/c/78141b8832e16d80d09cbefb4258612db0777a24
- https://git.kernel.org/stable/c/edc988613def90c5b558e025b1b423f48007be06
- https://git.kernel.org/stable/c/da4515fc8263c5933ed605e396af91079806dc45
- https://git.kernel.org/linus/d793458c45df2aed498d7f74145eab7ee22d25aa

- https://security-tracker.debian.org/tracker/CVE-2026-23372
- https://ubuntu.com/security/CVE-2026-23372
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12478

98

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31788
BDU:2026-12293

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Linux: от 2.6.37 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://xenbits.xen.org/xsa/advisory-482.html
- https://security-tracker.debian.org/tracker/CVE-2026-31788
- https://access.redhat.com/security/cve/CVE-2026-31788
- https://ubuntu.com/security/CVE-2026-31788
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/

- https://bdu.fstec.ru/vul/2026-12293

99

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23395
BDU:2026-12302

Идентификатор программной ошибки: CWE-1023 Неполное сравнение, связанное с отсутствующими факторами

Уязвимый продукт: Linux: от 5.7 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23395
- https://git.kernel.org/stable/c/fb4a3a26483f3ea2cd21c7a2f7c45d5670600465
- https://git.kernel.org/stable/c/2124d82fd25e1671bb3ceb37998af5aae5903e06
- https://git.kernel.org/stable/c/6b949a6b33cbdf621d9fc6f0c48ac00915dbf514
- https://git.kernel.org/stable/c/8d0d94f8ba5b3a0beec3b0da558b9bea48018117
- https://git.kernel.org/stable/c/e72ee455297b794b852e5cea8d2d7bb17312172a

- https://git.kernel.org/linus/5b3e2052334f2ff6d5200e952f4aa66994d09899
- https://security-tracker.debian.org/tracker/CVE-2026-23395
- https://access.redhat.com/security/cve/CVE-2026-23395
- https://ubuntu.com/security/CVE-2026-23395
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12302

100

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31414
BDU:2026-12268

Идентификатор программной ошибки: CWE-911 Некорректное обновление данных счетчика ссылок

Уязвимый продукт: Linux: от 2.6.30 до 6.1.167 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31414
- https://git.kernel.org/stable/c/847cb7fe26c5ce5dce0d1a41fac1ea488b7f1781
- https://git.kernel.org/stable/c/e7ccaa0a62a8ff2be5d521299ce79390c318d306
- https://git.kernel.org/stable/c/4bd1b3d839172724b33d8d02c5a4ff6a1c775417
- https://git.kernel.org/stable/c/b53294bff19e56ada2f230ceb8b1ffde61cc3817
- https://git.kernel.org/stable/c/3dfd3f7712b5a800f2ba632179e9b738076a51f0
- https://git.kernel.org/linus/f01794106042ee27e54af6fdf5b319a2fe3df94d

- https://security-tracker.debian.org/tracker/CVE-2026-31414
- https://access.redhat.com/security/cve/CVE-2026-31414
- https://ubuntu.com/security/CVE-2026-31414
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12268

Краткое описание: Получение конфиденциальной информации в Linux

Идентификатор уязвимости: CVE-2026-23456
BDU:2026-12252

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 2.6.17 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

101 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23456
- https://git.kernel.org/stable/c/41b417ff73a24b2c68134992cc44c88db27f482d
- https://git.kernel.org/stable/c/52235bf88159a1ef16434ab49e47e99c8a09ab20
- https://git.kernel.org/stable/c/774a434f8c9c8602a976b2536f65d0172a07f4d2
- https://git.kernel.org/stable/c/6bce72daeccca9aa1746e92d6c3d4784e71f2ebb
- https://git.kernel.org/stable/c/fb6c3596823ec5dd09c2123340330d7448f51a59

- https://git.kernel.org/linus/1e3a3593162c96e8a8de48b1e14f60c3b57fca8a
- https://security-tracker.debian.org/tracker/CVE-2026-23456
- https://access.redhat.com/security/cve/CVE-2026-23456
- https://ubuntu.com/security/CVE-2026-23456
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12252

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23455
BDU:2026-12238

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Linux: от 2.6.17 до 6.1.166 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 25.10
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

10
2

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-13 / 2026-08-13

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23455
- https://git.kernel.org/stable/c/495e97af9e7249ee02b72bb1d0848a6efc3700f4
- https://git.kernel.org/stable/c/f5e4f4e4cdb75ec36802059a94195a31f193da60
- https://git.kernel.org/stable/c/633e8f87dad32263f6a57dccdb873f042c062111
- https://git.kernel.org/stable/c/9d00fe7d6d7c5b5f1065a6e042b54f2e44bd6df8
- https://git.kernel.org/stable/c/b652b05d51003ac074b912684f9ec7486231717b

- https://git.kernel.org/linus/f173d0f4c0f689173f8cdac79991043a4a89bf66
- https://security-tracker.debian.org/tracker/CVE-2026-23455
- https://access.redhat.com/security/cve/CVE-2026-23455
- https://ubuntu.com/security/CVE-2026-23455
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12238

103

Краткое описание: Получение конфиденциальной информации в Linux

Идентификатор уязвимости: CVE-2026-31631
BDU:2026-12239

Идентификатор программной ошибки: CWE-805 Доступ к памяти за пределами буфера

Уязвимый продукт: Linux: от 6.16 до 6.18.22 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/794586789800b16dcbe235452494f4223ac80413
- https://git.kernel.org/stable/c/1c4422d8be81718ecb15d79aedff607323085201
- https://www.cve.org/CVERecord?id=CVE-2026-31631
- https://git.kernel.org/linus/f564af387c8c28238f8ebc13314c589d7ba8475d
- https://access.redhat.com/security/cve/CVE-2026-31631
- https://ubuntu.com/security/CVE-2026-31631
- https://bdu.fstec.ru/vul/2026-12239

10
4

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31464
BDU:2026-12240

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 2.6.27 до 5.10.253
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.7
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-31464
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-31464
- https://git.kernel.org/linus/61d099ac4a7a8fb11ebdb6e2ec8d77f38e77362f
- https://git.kernel.org/stable/c/394a1cac3c12fdd7d77f19ccfd222ab5ff87ef89
- https://git.kernel.org/stable/c/4ed727e35b0ab17d3eeeb1e8023768396e2be161

- https://git.kernel.org/stable/c/61d099ac4a7a8fb11ebdb6e2ec8d77f38e77362f
- https://git.kernel.org/stable/c/786f10b1966e485046839f992e89f2c18cbd1983
- https://git.kernel.org/stable/c/a007246cb6c9ebdc93dafbf63cc2d43d98f402cc
- https://git.kernel.org/stable/c/bae4df0a643fa7f84663473aa3082a9c2ed139db
- https://git.kernel.org/stable/c/d1466bf991b2343cf2ba8336e440c8faf3cbb780
- https://git.kernel.org/stable/c/d842348f8a00d5b1d7358f207eb34ffcf5b16df3
- https://nvd.nist.gov/vuln/detail/CVE-2026-31464
- https://security-tracker.debian.org/tracker/CVE-2026-31464
- https://ubuntu.com/security/CVE-2026-31464
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0820SE17
- https://www.cve.org/CVERecord?id=CVE-2026-31464
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12240

105

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31448
BDU:2026-12241

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Linux: от 2.6.22 до 6.1.167 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 25.10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31448
- https://git.kernel.org/stable/c/c66545e83a802c3851d9be27a41c0479dd29ff0c
- https://git.kernel.org/stable/c/ecc50bfca9b5c2ee6aeef998181689b80477367b
- https://git.kernel.org/stable/c/3a7667595bcad84da53fc156a418e110267c3412
- https://git.kernel.org/stable/c/416c86f30f91b4fb2642ef6b102596ca898f41a5
- https://git.kernel.org/stable/c/64f425b06b3bea9abc8977fd3982779b3ad070c9
- https://git.kernel.org/linus/5422fe71d26d42af6c454ca9527faaad4e677d6c

- https://security-tracker.debian.org/tracker/CVE-2026-31448
- https://access.redhat.com/security/cve/CVE-2026-31448
- https://ubuntu.com/security/CVE-2026-31448
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12241

106

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31636
BDU:2026-12242

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.16 до 6.18.22 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/7875f3d9777bd4e9892c4db830571ab8ac2044c0
- https://git.kernel.org/stable/c/20a188775a9a9982d1987e12660d9b44b40a6c99
- https://www.cve.org/CVERecord?id=CVE-2026-31636
- https://git.kernel.org/linus/3e3138007887504ee9206d0bfb5acb062c600025
- https://access.redhat.com/security/cve/cve-2026-31636
- https://ubuntu.com/security/CVE-2026-31636
- https://bdu.fstec.ru/vul/2026-12242

10
7

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31435
BDU:2026-12243

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Linux: от 6.12 до 6.18.20 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31435
- https://git.kernel.org/stable/c/3e5fd8f53b575ff2188f82071da19c977ca56c41
- https://git.kernel.org/stable/c/8f2f2bd128a8d9edbc1e785760da54ada3df69b7
- https://git.kernel.org/linus/7e57523490cd2efb52b1ea97f2e0a74c0fb634cd
- https://access.redhat.com/security/cve/CVE-2026-31435
- https://ubuntu.com/security/CVE-2026-31435
- https://bdu.fstec.ru/vul/2026-12243

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31570
BDU:2026-12244

Идентификатор программной ошибки: CWE-786 Доступ к разделу памяти перед началом буфера

Уязвимый продукт: Linux: от 5.4 до 5.10.252 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

10
8

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/84f8b76d24273175a22713e83e90874e1880d801
- https://git.kernel.org/stable/c/999ca48d55a8a46da21519db7e834e5867200379
- https://git.kernel.org/stable/c/e7c99348b0612b2bc02d5ce6ff9873261cc7605f
- https://git.kernel.org/stable/c/c4e8eaa75fa0b6bcbfa5356d6195c4ad0e05e57a
- https://git.kernel.org/stable/c/a025283d7f7404c739225e457fb99db2368bb544
- https://git.kernel.org/stable/c/54ecdf76a55e75c1f5085e440f8ab671a3283ef5

- https://git.kernel.org/stable/c/66b689efd08227da2c5ca49b58b30a95d23c695a
- https://www.cve.org/CVERecord?id=CVE-2026-31570
- https://git.kernel.org/linus/b9c310d72783cc2f30d103eed83920a5a29c671a
- https://security-tracker.debian.org/tracker/CVE-2026-31570
- https://access.redhat.com/security/cve/CVE-2026-31570
- https://ubuntu.com/security/CVE-2026-31570
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12244

10
9

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31609
BDU:2026-12245

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 6.19.1 до 6.19.13 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/a9940dcbe5cb92482c04efc7341039ddf7dbf607
- https://git.kernel.org/stable/c/f9a162c2bbcd0ac85bd07c5b37cf20286048b65c
- https://git.kernel.org/stable/c/22b7c1c619d808aec4cad3dc42103345e370d107
- https://www.cve.org/CVERecord?id=CVE-2026-31609
- https://git.kernel.org/linus/27b7c3e916218b5eb2ee350211140e961bfc49be
- https://access.redhat.com/security/cve/CVE-2026-31609
- https://ubuntu.com/security/CVE-2026-31609
- https://bdu.fstec.ru/vul/2026-12245

11
0

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31633
BDU:2026-12246

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Linux: от 6.16 до 6.18.22 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/1f864d9daaf622aeaa774404fd51e7d6a435b046
- https://git.kernel.org/stable/c/c1e242beb6b1efc3c286f617e8d940c8fbf2ed41
- https://www.cve.org/CVERecord?id=CVE-2026-31633
- https://git.kernel.org/linus/699e52180f4231c257821c037ed5c99d5eb0edb8
- https://access.redhat.com/security/cve/CVE-2026-31633
- https://ubuntu.com/security/CVE-2026-31633
- https://bdu.fstec.ru/vul/2026-12246

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31637
BDU:2026-12247

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: Linux: от 2.6.22 до 6.6.134 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 25.10
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

11 1 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/a149dcae23309df9de1c3b6b5d468610ef5ab7de
- https://git.kernel.org/stable/c/22f6258e7b31dba9bf88dce4e3ee7f0f20072e60
- https://git.kernel.org/stable/c/58fcd1b156152613ba00a064a129fb69507ddd7d
- https://git.kernel.org/stable/c/47073aab8a3a5a7b41c9bd37d2a3dcbeeccd6c8a
- https://www.cve.org/CVERecord?id=CVE-2026-31637
- https://git.kernel.org/linus/fe4447cd95623b1cfacc15f280aab73a6d7340b2

- https://security-tracker.debian.org/tracker/CVE-2026-31637
- https://access.redhat.com/security/cve/CVE-2026-31637
- https://ubuntu.com/security/CVE-2026-31637
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12247

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31649
BDU:2026-12248

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Linux: от 3.2 до 5.10.252 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 25.10
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

11
2 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/2c91b39912278d0878f9ba60ba04d2518b18a08d
- https://git.kernel.org/stable/c/a2b68a9a476b9544ff31f1fbcd5d80867a8a5e2f
- https://git.kernel.org/stable/c/b7b8012193fd98236d7ae05d4b553f010a77b2ef
- https://git.kernel.org/stable/c/10d12b9240ebf96c785f0e2e4228318cd5f3a3eb
- https://git.kernel.org/stable/c/6fca757c20396dc2e604dcc61922264e9e3dc803
- https://git.kernel.org/stable/c/275bdf762e82082f064e60a92448fa2ac43cf95b

- https://git.kernel.org/stable/c/513e06735f5be575b409d195822195348b164e48
- https://www.cve.org/CVERecord?id=CVE-2026-31649
- https://git.kernel.org/linus/51f4e090b9f87b40c21b6daadb5c06e6c0a07b67
- https://security-tracker.debian.org/tracker/CVE-2026-31649
- https://access.redhat.com/security/cve/CVE-2026-31649
- https://ubuntu.com/security/CVE-2026-31649
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12248

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31392
BDU:2026-12249

Идентификатор программной ошибки: CWE-488 Раскрытие (доступность) данных другим сессиям

Уязвимый продукт: Linux: от 2.6.36 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

11
3

Оценка CVSSv3: 8.1 AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31392
- https://git.kernel.org/stable/c/fd4547830720647d4af02ee50f883c4b1cca06e4
- https://git.kernel.org/stable/c/9229709ec8bf85ae7ca53aeee9aa14814cdc1bd2
- https://git.kernel.org/stable/c/d33cbf0bf8979d779900da9be2505d68d9d8da25
- https://git.kernel.org/stable/c/9ee803bfdba0cf739038dbdabdd4c02582c8f2b2
- https://git.kernel.org/stable/c/6e9ff1eb7feedcf46ff2d0503759960ab58e7775
- https://git.kernel.org/linus/12b4c5d98cd7ca46d5035a57bcd995df614c14e1

- https://security-tracker.debian.org/tracker/CVE-2026-31392
- https://access.redhat.com/security/cve/CVE-2026-31392
- https://ubuntu.com/security/CVE-2026-31392
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12249

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31436
BDU:2026-12250

Идентификатор программной ошибки: CWE-910 Использование недействительного файлового дескриптора

Уязвимый продукт: Linux: от 6.8 до 6.12.79 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 25.10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

11
4

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31436
- https://git.kernel.org/stable/c/e21da2ad8844585040fe4b82be1ad2fe99d40074
- https://git.kernel.org/stable/c/82656e8daf8de00935ae91b91bed43f4d6e0d644
- https://git.kernel.org/stable/c/0e4f43779d550e559be13a5cdb763bad92c4cc99
- https://git.kernel.org/linus/e1c9866173c5f8521f2d0768547a01508cb9ff27
- https://security-tracker.debian.org/tracker/CVE-2026-31436
- https://access.redhat.com/security/cve/CVE-2026-31436

- https://ubuntu.com/security/CVE-2026-31436
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12250

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31607
BDU:2026-12251

Идентификатор программной ошибки: CWE-805 Доступ к памяти за пределами буфера

Уязвимый продукт: Linux: от 2.6.39 до 6.12.82 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

115 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-18 / 2026-08-18

Ссылки на источник:

- https://git.kernel.org/stable/c/5e1c4ece08ccdc197177631f111845a2c68eede3
- https://git.kernel.org/stable/c/885c8591784da6314f9aa82fa460ac69f9f79e5f
- https://git.kernel.org/stable/c/8d155e2d1c4102f74f82a2bf9c016164bb0f7384
- https://git.kernel.org/stable/c/ef8ebb1c637b4cfb61a9dd2e013376774ee2033b
- https://git.kernel.org/stable/c/906f16a836de13fe61f49cdce2f66f2dbd14caf4
- https://www.cve.org/CVERecord?id=CVE-2026-31607

- https://git.kernel.org/linus/2ab833a16a825373aad2ba7d54b572b277e95b71
- https://security-tracker.debian.org/tracker/CVE-2026-31607
- https://access.redhat.com/security/cve/CVE-2026-31607
- https://ubuntu.com/security/CVE-2026-31607
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12251

Краткое описание: Перезапись произвольных файлов в Linux

Идентификатор уязвимости: CVE-2026-31393
BDU:2026-12344

Идентификатор программной ошибки: CWE-788 Доступ к областям памяти за пределами буфера

Уязвимый продукт: Linux: от 2.6.24 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Перезапись произвольных файлов

11
6 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31393
- https://git.kernel.org/stable/c/3b646516cba2ebc4b51a72954903326e7c1e443f
- https://git.kernel.org/stable/c/807bd1258453c4c83f6ae9dbc1e7b44860ff40d0
- https://git.kernel.org/stable/c/9aeacde4da0f02d42fd968fd32f245828b230171
- https://git.kernel.org/stable/c/e7ff754e339e3d5ce29aa9f95352d0186df8fbd9
- https://git.kernel.org/stable/c/db2872d054e467810078e2b9f440a5b326a601b2

- https://git.kernel.org/linus/dd815e6e3918dc75a49aaabac36e4f024d675101
- https://security-tracker.debian.org/tracker/CVE-2026-31393
- https://access.redhat.com/security/cve/CVE-2026-31393
- https://ubuntu.com/security/CVE-2026-31393
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12344

11
7

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23280
BDU:2026-12453

Идентификатор программной ошибки: CWE-680 Целочисленное переполнение, приводящее к переполнению буфера

Уязвимый продукт: Linux: от 6.18 до 6.18.16 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23280
- https://git.kernel.org/stable/c/1500b31db94374a6669e73ce94d6f71cf8e85e06
- https://git.kernel.org/stable/c/972bf4a23478fcb247b4f507d47a584bc8aea5bd
- https://git.kernel.org/linus/03808abb1d868aed7478a11a82e5bb4b3f1ca6d6
- https://bdu.fstec.ru/vul/2026-12453

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23281
BDU:2026-12454

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 2.6.24 до 6.1.166 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

118

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23281
- https://git.kernel.org/stable/c/3f9dec4a6d95d7f1f5e9e9dfdfa173c053bba8dc
- https://git.kernel.org/stable/c/3c5c818c78b03a1725f3dcd566865c77b48dd3a6
- https://git.kernel.org/stable/c/d0155fe68f31b339961cf2d4f92937d57e9384e6
- https://git.kernel.org/stable/c/ed7d30f90b77f73a47498686ede83f622b7e4f0d
- https://git.kernel.org/stable/c/a9f55b14486426d907459bced5825a25063bd922
- https://git.kernel.org/linus/03cc8f90d0537fcd4985c3319b4fafbf2e3fb1f0

- https://security-tracker.debian.org/tracker/CVE-2026-23281
- https://ubuntu.com/security/CVE-2026-23281
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12454

Краткое описание: Получение конфиденциальной информации в Linux

Идентификатор уязвимости: CVE-2026-23457
BDU:2026-12349

Идентификатор программной ошибки: CWE-681 Некорректное преобразование числовых типов

Уязвимый продукт: Linux: от 2.6.34 до 6.1.166 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

11
9

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-19 / 2026-08-19

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23457
- https://git.kernel.org/stable/c/b75209debb9adab287b3caa982f77788c1e15027
- https://git.kernel.org/stable/c/528b4509c9dfc272e2e92d811915e5211650d383
- https://git.kernel.org/stable/c/75fcaee5170e7dbbee778927134ef2e9568b4659
- https://git.kernel.org/stable/c/865dba58958c3a86786f89a501971ab0e3ec6ba9
- https://git.kernel.org/stable/c/d4f17256544cc37f6534a14a27a9dec3540c2015

- https://git.kernel.org/linus/fbce58e719a17aa215c724473fd5baaa4a8dc57c
- https://security-tracker.debian.org/tracker/CVE-2026-23457
- https://access.redhat.com/security/cve/CVE-2026-23457
- https://ubuntu.com/security/CVE-2026-23457
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12349

120

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63388
BDU:2026-12665

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Libevent: до 2.2.1-alpha включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-cvq5-vrvr-j338
- https://github.com/libevent/libevent/releases/tag/release-2.1.13-stable
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12665

121

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43384
BDU:2026-12677

Идентификатор программной ошибки: CWE-613 Некорректно настроенный срок действия сессий

Уязвимый продукт: Linux: от 6.7 до 6.12.77 включительно
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43384
- https://git.kernel.org/stable/c/8be6ed64966da48b6c4726918f106c18742a5125
- https://git.kernel.org/stable/c/a269cbdc442f8658bca35383e34b9d0b0ff95a1c
- https://git.kernel.org/stable/c/080b0e210088296dd50d6637c06c1db14246adfe
- https://git.kernel.org/linus/67edfec516d30d3e62925c397be4a1e5185802fc
- https://lore.kernel.org/linux-cve-announce/2026050834-CVE-2026-43384-d8ea@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43384
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12677

122

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43414
BDU:2026-12676

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 6.8.3 до 6.19.8 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43414
- https://git.kernel.org/stable/c/d48ea85463f5b34f7b92ea0a13eddf1ab993da7b
- https://git.kernel.org/linus/c0b7da13a04bd70ef6070bfb9ea85f582294560a
- https://lore.kernel.org/linux-cve-announce/2026050844-CVE-2026-43414-2950@gregkh/
- https://access.redhat.com/security/cve/cve-2026-43414
- https://bdu.fstec.ru/vul/2026-12676

123

Краткое описание: Выполнение произвольного кода в Zimbra Collaboration Suite

Идентификатор уязвимости: CVE-2026-73570
BDU:2026-12669

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Zimbra Collaboration Suite: до 10.1.20

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.9 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-73570
- https://github.com/BiuTrap/CVE-2026-73570?ysclid=mt8r31s9q2746084781
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-12669

12
4

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63495
BDU:2026-12666

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Libevent: от 2.2.0-alpha-dev до 2.2.2-alpha

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-qx89-wf2v-vgmx
- https://github.com/libevent/libevent/commit/291c4d1cd75695e898030ebd5c4ddf26c094077b
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12666

125

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63385
BDU:2026-12662

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Libevent: до 2.2.1-alpha включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-jcwh-pvf2-73p2
- https://github.com/libevent/libevent/releases/tag/release-2.1.13-stable
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12662

126

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43465
BDU:2026-12647

Идентификатор программной ошибки: CWE-911 Некорректное обновление данных счетчика ссылок

Уязвимый продукт: Linux: от 6.17.6 до 6.18.18 включительно
Red Hat Enterprise Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43465
- https://git.kernel.org/stable/c/7d7342a18fadcdb70a63b3c930dc63528ce51832
- https://git.kernel.org/stable/c/043bd62f748bc9fd98154037aa598cffbd3c667c
- https://git.kernel.org/linus/db25c42c2e1f9c0d136420fff5e5700f7e771a6f
- https://lore.kernel.org/linux-cve-announce/2026050802-CVE-2026-43465-291e@gregkh/
- https://access.redhat.com/security/cve/cve-2026-43465
- https://bdu.fstec.ru/vul/2026-12647

127

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63383
BDU:2026-12660

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Libevent: до 2.2.1-alpha включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-fj29-64w6-73h6
- https://github.com/libevent/libevent/releases/tag/release-2.1.13-stable
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12660

128

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63382
BDU:2026-12659

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Libevent: до 2.2.1-alpha включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-q39v-w2g7-gr8j
- https://github.com/libevent/libevent/releases/tag/release-2.1.13-stable
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12659

Краткое описание: Получение конфиденциальной информации в urllib

Идентификатор уязвимости: CVE-2026-55553
BDU:2026-12648

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: urllib: от 2.44.0 до 2.44.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

129

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/node-modules/urllib/security/advisories/GHSA-hq3h-g68c-hp78
- https://github.com/node-modules/urllib/commit/7c86c465883ebd3dea5109c87d7bbe3b00960a16
- https://github.com/node-modules/urllib/commit/811a8d56e64e540bf6a19bf8b3737692f05d5c46
- https://github.com/node-modules/urllib/pull/812 GitHub, Inc.
- https://github.com/node-modules/urllib/pull/813 GitHub, Inc.
- https://github.com/node-modules/urllib/releases/tag/v2.44.1
- https://github.com/node-modules/urllib/releases/tag/v4.9.1
- https://bdu.fstec.ru/vul/2026-12648

130

Краткое описание: Отказ в обслуживании в Libevent

Идентификатор уязвимости: CVE-2026-63384
BDU:2026-12661

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Libevent: до 2.2.1-alpha включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/libevent/libevent/security/advisories/GHSA-45c6-qx49-89m8
- https://github.com/libevent/libevent/releases/tag/release-2.1.13-stable
- https://github.com/libevent/libevent/releases/tag/release-2.2.2-alpha
- https://bdu.fstec.ru/vul/2026-12661

131

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-78675
BDU:2026-12716

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: GitPython: до 3.1.58 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-7833-fr7j-v32q
- https://bdu.fstec.ru/vul/2026-12716

132

Краткое описание: Повышение привилегий в SQL Server ODBC driver

Идентификатор уязвимости: CVE-2026-42990
BDU:2026-12719

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 23H2: до 10.0.22631.7376
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42990
- https://bdu.fstec.ru/vul/2026-12719

133

Краткое описание: Выполнение произвольного кода в Windows Bluetooth Port Driver

Идентификатор уязвимости: CVE-2026-42975
BDU:2026-12718

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42975
- https://bdu.fstec.ru/vul/2026-12718

134

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43426
BDU:2026-12727

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.0 до 5.10.252 включительно
Debian GNU/Linux: 13
Альт 8 СП: -
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/6287e0c01ccb818e7214f88d885ffb7c9e81b0e0
- https://www.cve.org/CVERecord?id=CVE-2026-43426
- https://git.kernel.org/stable/c/c7012fc73dab4829404fedeeaa8531f12ac8545f
- https://git.kernel.org/stable/c/51afaf919bbaacdd9cc9e146033ae0a743a42dd7
- https://git.kernel.org/stable/c/1899edac312ef17a7234851686e8a703f56d0a84
- https://git.kernel.org/stable/c/9c6159d5b72d5fc265cce5da04f27d730b552e69
- https://git.kernel.org/stable/c/0b7d11fd6e742ecc0b1eca44b4f0b93140c74bae
- https://git.kernel.org/stable/c/6ffe44f022c95b1b29c691d2169c5abc046f7580

- https://git.kernel.org/linus/3cbc242b88c607f55da3d0d0d336b49bf1e20412
- https://lore.kernel.org/linux-cve-announce/2026050849-CVE-2026-43426-eef1@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43426
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12727

135

Краткое описание: Повышение привилегий в Windows Secure Kernel Mode

Идентификатор уязвимости: CVE-2026-42982
BDU:2026-12720

Идентификатор программной ошибки: CWE-1023 Неполное сравнение, связанное с отсутствующими факторами

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 23H2: до 10.0.22631.7376
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42982
- https://bdu.fstec.ru/vul/2026-12720

136

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43318
BDU:2026-12728

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 5.7 до 6.12.74 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/82a7ea35a1526bef8ae170c33ff80e5db7728961
- https://www.cve.org/CVERecord?id=CVE-2026-43318
- https://git.kernel.org/stable/c/89a9389ad70d3c69538e59d87df67d407aef4c26
- https://git.kernel.org/stable/c/3307459eb3583115264421e859858d1f90f3694a
- https://git.kernel.org/linus/b18fc0ab837381c1a6ef28386602cd888f2d9edf
- https://lore.kernel.org/linux-cve-announce/2026050818-CVE-2026-43318-79ab@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43318
- https://access.redhat.com/security/cve/cve-2026-43318

- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12728

137

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43185
BDU:2026-12732

Идентификатор программной ошибки: CWE-704 Некорректное преобразование или приведение типов

Уязвимый продукт: Linux: от 5.15 до 6.18.15 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43185
- https://git.kernel.org/stable/c/ceae058eb707ddd0d68f0872f9d9f23b7c30c37b
- https://git.kernel.org/stable/c/55abc475d096da4a5356b6efb0cfdc6156bc1550
- https://git.kernel.org/linus/6b4f875aac344cdd52a1f34cc70ed2f874a65757
- https://lore.kernel.org/linux-cve-announce/2026050640-CVE-2026-43185-55a5@gregkh/
- https://bdu.fstec.ru/vul/2026-12732

13
8

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43098
BDU:2026-12730

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 5.11 до 6.6.135 включительно
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43098
- https://git.kernel.org/stable/c/d8c2aa3c4a1ec530a485e46a1c4f1a118bb00156
- https://git.kernel.org/stable/c/7c31f7a599cf00fad3c204092a91a924126c67e4
- https://git.kernel.org/stable/c/6d931680a9851481c3243689488eafed08eeff71
- https://git.kernel.org/stable/c/09822d3d6f68a0cdc4626e0c507324a4927f55a9
- https://git.kernel.org/linus/5c14a19d5b1645cce1cb1252833d70b23635b632
- https://lore.kernel.org/linux-cve-announce/2026050620-CVE-2026-43098-960f@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43098
- https://altsp.su/obnovleniya-bezopasnosti/

- https://bdu.fstec.ru/vul/2026-12730

139

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43380
BDU:2026-12731

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.16 до 6.1.166 включительно
Debian GNU/Linux: 13
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43380
- https://git.kernel.org/stable/c/a0fc1b9c738fba231f190ab960c83202722efee5
- https://git.kernel.org/stable/c/c59090c50f62a17129fc4c5407bc4071305a9e82
- https://git.kernel.org/stable/c/52db5ef163c96f916d424e472fb17aadc35a9f7a
- https://git.kernel.org/stable/c/b48a0f8d4541a4f6651dc9a64430ce9fdf5c120b
- https://git.kernel.org/stable/c/73a7a345816946d276ad2c46c8bb771de67cfc46
- https://git.kernel.org/stable/c/24a7b9daa103fa963b3fd37d8805b23e01621976
- https://git.kernel.org/linus/25dd70a03b1f5f3aa71e1a5091ecd9cd2a13ee43
- https://lore.kernel.org/linux-cve-announce/2026050832-CVE-2026-43380-d98b@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-43380
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12731

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43376
BDU:2026-12733

Идентификатор программной ошибки: CWE-667 Некорректная блокировка

Уязвимый продукт: Linux: от 6.14.4 до 6.18.18 включительно
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

140

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/ce8507ee82c888126d8e7565e27c016308d24cde
- https://www.cve.org/CVERecord?id=CVE-2026-43376
- https://git.kernel.org/stable/c/302fef75512b2c8329a3f5efab1ae7ba2562387a
- https://git.kernel.org/stable/c/08aa9f3c8cf4d0bee44df540dfe34e8d64069f2c
- https://git.kernel.org/stable/c/1d6abf145615dbfe267ce3b0a271f95e3780e18e
- https://git.kernel.org/linus/1dfd062caa165ec9d7ee0823087930f3ab8a6294
- https://lore.kernel.org/linux-cve-announce/2026050831-CVE-2026-43376-e32d@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43376
- https://bdu.fstec.ru/vul/2026-12733

141

Краткое описание: Отказ в обслуживании в kin-openapi

Идентификатор уязвимости: CVE-2026-77354
BDU:2026-12709

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: kin-openapi: от 0.124.0 до 0.142.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/getkin/kin-openapi/security/advisories/GHSA-xhj3-7xw9-vr34
- https://github.com/getkin/kin-openapi/pull/923
- https://github.com/getkin/kin-openapi/releases/tag/v0.142.0
- https://bdu.fstec.ru/vul/2026-12709

142

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43460
BDU:2026-12729

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 6.14 до 6.18.18 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43460
- https://git.kernel.org/stable/c/b6051f2bdd4bd3dde85b68558edd3a6843489221
- https://git.kernel.org/stable/c/85fb53351e6a3b921357a2178671e847a087e400
- https://git.kernel.org/linus/111e2863372c322e836e0c896f6dd9cf4ee08c71
- https://lore.kernel.org/linux-cve-announce/2026050801-CVE-2026-43460-5893@gregkh/
- https://bdu.fstec.ru/vul/2026-12729

143

Краткое описание: Отказ в обслуживании в kin-openapi

Идентификатор уязвимости: CVE-2026-76905
BDU:2026-12708

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: kin-openapi: от 0.10.0 до 0.141.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/getkin/kin-openapi/security/advisories/GHSA-mmfr-pmjx-hw9w
- https://github.com/getkin/kin-openapi/releases/tag/v0.141.0
- https://bdu.fstec.ru/vul/2026-12708

144

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73939
BDU:2026-12699

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 3.2.20

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73939
- https://bdu.fstec.ru/vul/2026-12699

145

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-78676
BDU:2026-12705

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: GitPython: до 3.1.58 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-284h-m62q-gf8w
- https://bdu.fstec.ru/vul/2026-12705

146

Краткое описание: Получение конфиденциальной информации в Netty

Идентификатор уязвимости: CVE-2026-61798
BDU:2026-12706

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: Netty: до 0.0.22.Final включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/advisories/GHSA-2mc4-j865-9q4r
- https://www.kodemsecurity.com/cve-archive/cve-2026-61798
- https://bdu.fstec.ru/vul/2026-12706

147

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73931
BDU:2026-12680

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73931
- https://bdu.fstec.ru/vul/2026-12680

148

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73929
BDU:2026-12682

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73929
- https://bdu.fstec.ru/vul/2026-12682

149

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73927
BDU:2026-12683

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 3.2.20

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73927
- https://bdu.fstec.ru/vul/2026-12683

150

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73925
BDU:2026-12684

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 1.4.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73925
- https://bdu.fstec.ru/vul/2026-12684

151

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73924
BDU:2026-12685

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 1.4.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73924
- https://bdu.fstec.ru/vul/2026-12685

152

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73922
BDU:2026-12686

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 1.4.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73922
- https://bdu.fstec.ru/vul/2026-12686

153

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73921
BDU:2026-12687

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 1.4.20

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73921
- https://bdu.fstec.ru/vul/2026-12687

154

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73920
BDU:2026-12688

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73920
- https://bdu.fstec.ru/vul/2026-12688

155

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73917
BDU:2026-12690

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73917
- https://bdu.fstec.ru/vul/2026-12690

156

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73930
BDU:2026-12681

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73930
- https://bdu.fstec.ru/vul/2026-12681

157

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73934
BDU:2026-12693

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 3.2.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73934
- https://bdu.fstec.ru/vul/2026-12693

158

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73935
BDU:2026-12694

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73935
- https://bdu.fstec.ru/vul/2026-12694

159

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73936
BDU:2026-12695

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73936
- https://bdu.fstec.ru/vul/2026-12695

160

Краткое описание: Отказ в обслуживании в Helidon

Идентификатор уязвимости: CVE-2026-73937
BDU:2026-12696

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73937
- https://bdu.fstec.ru/vul/2026-12696

161

Краткое описание: Получение конфиденциальной информации в Helidon

Идентификатор уязвимости: CVE-2026-73938
BDU:2026-12697

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 4.5.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73938
- https://bdu.fstec.ru/vul/2026-12697

162

Краткое описание: Запись локальных файлов в GitPython

Идентификатор уязвимости: CVE-2026-78677
BDU:2026-12704

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: GitPython: до 3.1.58 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Запись локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-8mcc-hrx5-hvxc
- https://bdu.fstec.ru/vul/2026-12704

163	**Краткое описание:** Выполнение произвольного кода в GeoTools **Идентификатор уязвимости:** CVE-2026-76904 BDU:2026-12700 **Идентификатор программной ошибки:** CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода) **Уязвимый продукт:** GeoTools: до 33.6 **Категория уязвимого продукта:** Универсальные компоненты и библиотеки **Способ эксплуатации:** Инъекция. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **Оценка CVSSv4:** Не определено **Вектор атаки:** Сетевой **Взаимодействие с пользователем:** Отсутствует **Дата выявления / Дата обновления:** 2026-08-27 / 2026-08-27 **Ссылки на источник:** • https://github.com/geotools/geotools/security/advisories/GHSA-mqjf-5f49-2fjh • https://osgeo-org.atlassian.net/browse/GEOT-7589 • https://osgeo-org.atlassian.net/browse/GEOT-7958 • https://osgeo-org.atlassian.net/browse/GEOT-7959 • https://github.com/geotools/geotools/commit/d821c4d321dd91c22e31fcd5b1ce676645da5176 • https://github.com/geotools/geotools/pull/5829 • https://github.com/geotools/geotools/releases/tag/33.6 • https://github.com/geotools/geotools/releases/tag/34.5 • https://github.com/geotools/geotools/releases/tag/35.1 • https://gist.github.com/portbuster1337

- https://github.com/YonLiud/CVE-2026-76904
- https://bdu.fstec.ru/vul/2026-12700

164

Краткое описание: Выполнение произвольного кода в Python NLTK library

Идентификатор уязвимости: CVE-2026-79657
BDU:2026-12702

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: NLTK: до 3.10.2 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/nltk/nltk/security/advisories/GHSA-x99w-6fgc-pmfw
- https://bdu.fstec.ru/vul/2026-12702

165

Краткое описание: Чтение локальных файлов в Python NLTK library

Идентификатор уязвимости: CVE-2026-78682
BDU:2026-12703

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: NLTK: до 3.10.2 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://github.com/nltk/nltk/security/advisories/GHSA-6ww7-3frv-cqxh
- https://bdu.fstec.ru/vul/2026-12703

166

Краткое описание: Выполнение произвольного кода в Helidon

Идентификатор уязвимости: CVE-2026-73916
BDU:2026-12691

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helidon: 3.2.18

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-20 / 2026-08-20

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspuaug2026.html
- https://www.oracle.com/security-alerts/cspuaug2026verbose.html
- https://app.opencve.io/cve/CVE-2026-73916
- https://bdu.fstec.ru/vul/2026-12691

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31563
BDU:2026-12835

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.16.6 до 6.18.21
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.7
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

167

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-31563
- https://security-tracker.debian.org/tracker/CVE-2026-31563
- https://git.kernel.org/linus/647b8a2fe474474704110db6bd07f7a139e621eb
- https://git.kernel.org/stable/c/647b8a2fe474474704110db6bd07f7a139e621eb
- https://git.kernel.org/stable/c/78c8b090a3d5c1689dc989861b0163180db2b3f8
- https://git.kernel.org/stable/c/92e7081f0c79d9073087e54bab745bb184192c2e
- https://git.kernel.org/stable/c/984350b37372f79f71d4f0a5264c640e40daf9ce

- https://git.kernel.org/stable/c/ca4d05afb4683d685bb2c6fccae4386c478f524a
- https://git.kernel.org/stable/c/f4bc91398b57973028432832 2365afa77a9d568f
- https://github.com/torvalds/linux/commit/92e7081f0c79d9073087e54bab745bb184192c2e
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0820SE17
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-31563
- https://ubuntu.com/security/CVE-2026-31563
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12835

168

Краткое описание: Отказ в обслуживании в vorbis-tools

Идентификатор уязвимости: CVE-2026-34253
BDU:2026-12840

Идентификатор программной ошибки: CWE-124 Запись данных в область перед началом буфера

Уязвимый продукт: vorbis-tools: до 1.4.3 включительно
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-34253
- https://security-tracker.debian.org/tracker/CVE-2026-34253
- https://github.com/xiph/vorbis-tools/archive/refs/tags/v1.4.3.tar.gz
- https://github.com/xiph/vorbis-tools/blob/0b3fbf42eb3897d32f4a75baa2dc915a4ca45e8e/ogg123/remote.c#L153
- https://gitlab.xiph.org/xiph/vorbis-tools/-/commit/4bb4fb33b25949178179f689db9afb477abeb572
- https://gitlab.xiph.org/xiph/vorbis-tools/-/commit/cfc497a442f51fb4885e132deaf2e0ba067bd280
- https://gitlab.xiph.org/xiph/vorbis-tools/-/work_items/2332
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0820SE17
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-34253

- https://bdu.fstec.ru/vul/2026-12840

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31779
BDU:2026-12836

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.7 до 6.12.81
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.7
АЛЬТ СП 10: -

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

169 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-31779
- https://security-tracker.debian.org/tracker/CVE-2026-31779
- https://git.kernel.org/linus/744fabc338e87b95c4d1ff7c95bc8c0f834c6d99
- https://git.kernel.org/stable/c/744fabc338e87b95c4d1ff7c95bc8c0f834c6d99
- https://git.kernel.org/stable/c/ca0e9491b98ca4c5b44204b0b3dd8062a3b5fba2
- https://git.kernel.org/stable/c/dd90880eb5ec5442b37eb2b95688f4a63f4883e3

- https://git.kernel.org/stable/c/e67d8c626ace80b0fa2b48c8ec0a46b508c93442
- https://git.kernel.org/stable/c/f6abac936a0dfd31d6c3e49205ec0ee75a8f887f
- https://git.kernel.org/stable/c/ffbed27ba15ef80d1c622eeedbfef03e501ae134
- https://github.com/torvalds/linux/commit/dd90880eb5ec5442b37eb2b95688f4a63f4883e3
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0820SE17
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-31779
- https://ubuntu.com/security/CVE-2026-31779
- https://access.redhat.com/security/cve/CVE-2026-31779
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-12836

170

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43402
BDU:2026-12810

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.14 до 6.18.18 включительно
Red Hat Enterprise Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43402
- https://git.kernel.org/stable/c/4729c7b00a347fd37d0cbc265b85f2884c3e06b6
- https://git.kernel.org/stable/c/5a591d7a5e48d30100943940a30a6ab41b15c672
- https://git.kernel.org/linus/28aaa9c39945b7925a1cc1d513c8f21ed38f5e4f
- https://lore.kernel.org/linux-cve-announce/2026050840-CVE-2026-43402-28f0@gregkh/
- https://access.redhat.com/security/cve/cve-2026-43402
- https://bdu.fstec.ru/vul/2026-12810

171

Краткое описание: Выполнение произвольного кода в Windows TCP/IP

Идентификатор уязвимости: CVE-2026-62792
BDU:2026-12767

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62792
- https://bdu.fstec.ru/vul/2026-12767

172

Краткое описание: Повышение привилегий в Windows Shell

Идентификатор уязвимости: CVE-2026-62770
BDU:2026-12765

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62770
- https://bdu.fstec.ru/vul/2026-12765

173

Краткое описание: Повышение привилегий в Windows User-Mode Power Service

Идентификатор уязвимости: CVE-2026-62721
BDU:2026-12757

Идентификатор программной ошибки: CWE-1052 Чрезмерное использование жестко закодированных литералов для инициализации

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62721
- https://bdu.fstec.ru/vul/2026-12757

Краткое описание: Повышение привилегий в Windows Sensor Data Service

Идентификатор уязвимости: CVE-2026-61355
BDU:2026-12756

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

17
4

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-61355
- https://bdu.fstec.ru/vul/2026-12756

175

Краткое описание: Повышение привилегий в Windows Accessibility Infrastructure

Идентификатор уязвимости: CVE-2026-61358
BDU:2026-12751

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-61358
- https://bdu.fstec.ru/vul/2026-12751

176

Краткое описание: Выполнение произвольного кода в Remote Desktop Client

Идентификатор уязвимости: CVE-2026-61363
BDU:2026-12750

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-61363
- https://bdu.fstec.ru/vul/2026-12750

177

Краткое описание: Повышение привилегий в Windows Device Association Service

Идентификатор уязвимости: CVE-2026-62710
BDU:2026-12747

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62710
- https://bdu.fstec.ru/vul/2026-12747

178

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-62711
BDU:2026-12746

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62711
- https://bdu.fstec.ru/vul/2026-12746

179

Краткое описание: Выполнение произвольного кода в RPC Runtime Library

Идентификатор уязвимости: CVE-2026-62781
BDU:2026-12745

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62781
- https://bdu.fstec.ru/vul/2026-12745

180

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-62797
BDU:2026-12743

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62797
- https://bdu.fstec.ru/vul/2026-12743

181

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-62876
BDU:2026-12742

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62876
- https://bdu.fstec.ru/vul/2026-12742

182

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-68816
BDU:2026-12792

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Office Online Server: до 16.0.10417.20175
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.112.26081010
Microsoft Excel 2016: до 16.0.5565.1001
Microsoft Office LTSC 2024: до 16.112.26081010
Microsoft Office 2019: -
Microsoft Office 365: до 16.112.26081010

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68816
- https://bdu.fstec.ru/vul/2026-12792

183

Краткое описание: Отказ в обслуживании в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20313
BDU:2026-12789

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Catalyst SD-WAN Manager: 26.1.1.2_LI_Images
Cisco Catalyst SD-WAN Controller: 26.1.1.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K
- https://github.com/HORKimhab/Cisco-CVE-2026-20303-More
- https://bdu.fstec.ru/vul/2026-12789

184

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-68801
BDU:2026-12788

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Office Online Server: до 16.0.10417.20175
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.112.26081010
Microsoft Excel 2016: до 16.0.5565.1001
Microsoft Office LTSC 2024: до 16.112.26081010
Microsoft Office 2019: -
Microsoft Office 365: до 16.112.26081010

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68801
- https://bdu.fstec.ru/vul/2026-12788

185

Краткое описание: Выполнение произвольного кода в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20312
BDU:2026-12787

Идентификатор программной ошибки: CWE-312 Хранение важных данных в незашифрованном виде

Уязвимый продукт: Catalyst SD-WAN Manager: 26.1.1.2_LI_Images
Cisco Catalyst SD-WAN Controller: 26.1.1.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K
- https://github.com/HORKimhab/Cisco-CVE-2026-20303-More
- https://bdu.fstec.ru/vul/2026-12787

186

Краткое описание: Получение конфиденциальной информации в Python NLTK library

Идентификатор уязвимости: CVE-2026-79674
BDU:2026-12782

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: NLTK: до 3.10.2 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://github.com/nltk/nltk/security/advisories/GHSA-3gq4-3j92-5w49
- https://bdu.fstec.ru/vul/2026-12782

187

Краткое описание: Выполнение произвольного кода в Balbooa Forms

Идентификатор уязвимости: CVE-2026-56291
BDU:2026-13205

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: Balbooa Forms: до 2.4.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://www.balbooa.com/joomla-forms
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-56291
- https://mysites.guru/blog/balbooa-forms-unauthenticated-file-upload-flaw/
- https://bdu.fstec.ru/vul/2026-13205

188

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43208
BDU:2026-13249

Идентификатор программной ошибки: CWE-805 Доступ к памяти за пределами буфера

Уязвимый продукт: Linux: от 6.18 до 6.18.15 включительно

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43208
- https://git.kernel.org/stable/c/ed712dc0d64dee5f0d05e4d8ca57711f8a9c850c
- https://git.kernel.org/linus/8a8a9fac9efa6423fd74938b940cb7d731780718
- https://git.kernel.org/stable/c/5455a232edea6b946b99449f15ca771a8874a5a6
- https://lore.kernel.org/linux-cve-announce/2026050648-CVE-2026-43208-cc6f@gregkh/
- https://bdu.fstec.ru/vul/2026-13249

189

Краткое описание: Выполнение произвольного кода в DIAFAN.CMS

Идентификатор уязвимости: BDU:2026-13254

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: DIAFAN.CMS: 7.5.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-09-01

Ссылки на источник:

- https://www.diafan.ru/news/diafancms-765-obnovlenie-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-13254

190

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-72137
BDU:2026-13147

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: до 7.2 rc4
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://git.kernel.org/stable/c/226f4a490d1a938fc838d8f8c46a4eca864c0d78
- https://git.kernel.org/stable/c/5b0c4c916f202b8fd13d12afb6af62b385622f81
- https://git.kernel.org/stable/c/a8a7e6a9ff8a4c1f067694ddbd44be67fdf36693
- https://git.kernel.org/stable/c/d0a4dc7efa825bce60a8da8f7d43c864a159abde
- https://security-tracker.debian.org/tracker/CVE-2026-72137
- https://ubuntu.com/security/CVE-2026-72137
- https://github.com/NebuSec/CyberMeowfia/tree/main/security-research/Linux-CVE-2026-72137-ubuntu-7.0.0-28
- https://bdu.fstec.ru/vul/2026-13147

191

Краткое описание: Обход безопасности в Rsync

Идентификатор уязвимости: CVE-2026-70463
BDU:2026-13148

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Rsync: от 3.1.0 до 3.4.4 включительно
АЛЬТ СП 10: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/RsyncProject/rsync/security/advisories/GHSA-pfj8-79vq-xgvr
- https://github.com/RsyncProject/rsync/releases/tag/v3.5.0
- https://github.com/Fyyre/CVE-2026-70463
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-13148

192

Краткое описание: Обход безопасности в SeaweedFS

Идентификатор уязвимости: CVE-2026-77368
BDU:2026-13150

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SeaweedFS: 4.39

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/seaweedfs/seaweedfs/commit/fa549e9c83b7799d512157d728f52052912831af
- https://github.com/seaweedfs/seaweedfs/commit/ce82e3a057080162a9fba11889157d2255815f71
- https://github.com/seaweedfs/seaweedfs/security/advisories/GHSA-99q7-x53r-6j4g
- https://bdu.fstec.ru/vul/2026-13150

Краткое описание: Отказ в обслуживании в Windows iSCSI Target Service

Идентификатор уязвимости: CVE-2026-65681
BDU:2026-13287

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

193

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65681
- https://bdu.fstec.ru/vul/2026-13287

194

Краткое описание: Выполнение произвольного кода в Windows Secure Socket Tunneling Protocol

Идентификатор уязвимости: CVE-2026-62889
BDU:2026-13291

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62889
- https://bdu.fstec.ru/vul/2026-13291

195

Краткое описание: Выполнение произвольного кода в Windows iSCSI Target Service

Идентификатор уязвимости: CVE-2026-65679
BDU:2026-13288

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65679
- https://bdu.fstec.ru/vul/2026-13288

196

Краткое описание: Повышение привилегий в Remote Access API

Идентификатор уязвимости: CVE-2026-65671
BDU:2026-13289

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65671
- https://bdu.fstec.ru/vul/2026-13289

Краткое описание: Повышение привилегий в Windows DWM Core Library

Идентификатор уязвимости: CVE-2026-62888
BDU:2026-13290

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

19
7

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62888
- https://bdu.fstec.ru/vul/2026-13290

198

Краткое описание: Повышение привилегий в Windows GDI+

Идентификатор уязвимости: CVE-2026-62890
BDU:2026-13292

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62890
- https://bdu.fstec.ru/vul/2026-13292

199

Краткое описание: Выполнение произвольного кода в Windows Reliable Multicast Transport Driver

Идентификатор уязвимости: CVE-2026-62816
BDU:2026-13301

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62816
- https://bdu.fstec.ru/vul/2026-13301

200

Краткое описание: Выполнение произвольного кода в Remote Desktop Client

Идентификатор уязвимости: CVE-2026-62824
BDU:2026-13296

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62824
- https://bdu.fstec.ru/vul/2026-13296

201

Краткое описание: Выполнение произвольного кода в Windows DNS Server

Идентификатор уязвимости: CVE-2026-62820
BDU:2026-13297

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62820

- https://bdu.fstec.ru/vul/2026-13297

Краткое описание: Выполнение произвольного кода в Windows Active Directory Certificate Services

Идентификатор уязвимости: CVE-2026-62818
BDU:2026-13298

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

20
2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62818
- https://bdu.fstec.ru/vul/2026-13298

203

Краткое описание: Выполнение произвольного кода в Windows DNS Server

Идентификатор уязвимости: CVE-2026-62817
BDU:2026-13300

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62817
- https://bdu.fstec.ru/vul/2026-13300

204

Краткое описание: Повышение привилегий в Desktop Window Manager

Идентификатор уязвимости: CVE-2026-65787
BDU:2026-13286

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65787
- https://bdu.fstec.ru/vul/2026-13286

205

Краткое описание: Выполнение произвольного кода в Windows DNS Server

Идентификатор уязвимости: CVE-2026-62878
BDU:2026-13294

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62878
- https://bdu.fstec.ru/vul/2026-13294

206

Краткое описание: Выполнение произвольного кода в Windows DNS Server

Идентификатор уязвимости: CVE-2026-65789
BDU:2026-13285

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65789
- https://bdu.fstec.ru/vul/2026-13285

Краткое описание: Выполнение произвольного кода в Windows Device Health Attestation

Идентификатор уязвимости: CVE-2026-71331
BDU:2026-13278

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Windows 10 1809: до 10.0.17763.9121
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

20
7

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-71331
- https://bdu.fstec.ru/vul/2026-13278

208

Краткое описание: Повышение привилегий в Windows Message Queuing

Идентификатор уязвимости: CVE-2026-65790
BDU:2026-13283

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65790
- https://bdu.fstec.ru/vul/2026-13283

209

Краткое описание: Повышение привилегий в Microsoft Windows Storage Port Driver

Идентификатор уязвимости: CVE-2026-65814
BDU:2026-13284

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65814
- https://bdu.fstec.ru/vul/2026-13284

Краткое описание: Получение конфиденциальной информации в NRF RegisterNFInstance

Идентификатор уязвимости: CVE-2026-55068
BDU:2026-13266

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: free5GC: до 4.2.2 включительно
nrf: до 1.4.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

210

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/free5gc/free5gc/issues/1056
- https://github.com/free5gc/free5gc/releases/tag/v4.2.3
- https://github.com/free5gc/free5gc/security/advisories/GHSA-x8mj-6p3q-g5pp
- https://github.com/free5gc/nrf/commit/bda0cf75be5556bb4c758c8b34710f3fe6bbe3ea
- https://github.com/free5gc/nrf/commit/fcd3cfaa27cc4dc17172ee0c4c3e0a3a696297c6
- https://github.com/free5gc/nrf/pull/90
- https://github.com/free5gc/nrf/releases/tag/v1.4.5
- https://bdu.fstec.ru/vul/2026-13266

211

Краткое описание: Выполнение произвольного кода в PHP pimcore

Идентификатор уязвимости: CVE-2026-55220
BDU:2026-13267

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: pimcore: до 11.5.18 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/pimcore/pimcore/commit/b184c01bf11e213e601d965b4e96c8bb7248e980
- https://github.com/pimcore/pimcore/releases/tag/v12.3.10
- https://github.com/pimcore/pimcore/releases/tag/v2026.1.6
- https://github.com/pimcore/pimcore/security/advisories/GHSA-w23p-wrp7-ch38
- https://bdu.fstec.ru/vul/2026-13267

21
2

Краткое описание: Чтение локальных файлов в Bifrost

Идентификатор уязвимости: CVE-2026-55245
BDU:2026-13268

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: Bifrost: до 1.5.15 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/maximhq/bifrost/commit/54ec431fc5255ff42c36420d88549477e0b33d89
- https://github.com/maximhq/bifrost/releases/tag/core/v1.5.17
- https://github.com/maximhq/bifrost/security/advisories/GHSA-w98g-5w9p-p3rc
- https://bdu.fstec.ru/vul/2026-13268

213

Краткое описание: Отказ в обслуживании в gix-pack

Идентификатор уязвимости: CVE-2026-82254
BDU:2026-13270

Идентификатор программной ошибки: CWE-248 Необработанное исключение

Уязвимый продукт: gix-pack: до 0.68.0 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://github.com/GitoxideLabs/gitoxide/security/advisories/GHSA-x494-mj8g-cj27
- https://bdu.fstec.ru/vul/2026-13270

214

Краткое описание: Выполнение произвольного кода в Apache Log4j Core

Идентификатор уязвимости: BDU:2026-13271

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Apache Log4j Core: от 2.8.0 до 2.26.1
Log4j-api: от 2.11.0 до 2.26.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://www.broadcom.com/support/security-center/protection-bulletin/unauthenticated-rce-vulnerability-in-apache-log4j2-issue-4255
- https://cybersecuritynews.com/new-apache-log4j2-flaw/
- https://bdu.fstec.ru/vul/2026-13271

215

Краткое описание: Повышение привилегий в Avast Antivirus

Идентификатор уязвимости: BDU:2026-13272

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Avast Antivirus: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://git.projectnightcrawler.dev/NightmareEclipse/PrettyPrague?utm_source=Securitylab.ru
- https://techora.ru/news/opublikovan-poc-dlya-uyazvimosti-prettyprague-v-2026-08-31
- https://github.com/MSNightmare/PrettyPrague
- https://bdu.fstec.ru/vul/2026-13272

21
6

Краткое описание: Выполнение произвольного кода в su-exec

Идентификатор уязвимости: CVE-2026-82457
BDU:2026-13269

Идентификатор программной ошибки: CWE-681 Некорректное преобразование числовых типов

Уязвимый продукт: su-exec: 0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://gist.github.com/thesmartshadow/ed96e2a88643c34a247c9b7cf9e311be
- https://github.com/ncopa/su-exec
- https://github.com/ncopa/su-exec/blob/89c016e6e08749d583efdeda04b9f73e1218e253/su-exec.c
- https://www.vulncheck.com/advisories/su-exec-through-0.3-privilege-escalation-via-numeric-user-id
- https://bdu.fstec.ru/vul/2026-13269

217

Краткое описание: Повышение привилегий в Windows Installer

Идентификатор уязвимости: CVE-2026-70346
BDU:2026-13276

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70346
- https://bdu.fstec.ru/vul/2026-13276

218

Краткое описание: Повышение привилегий в Windows Installer

Идентификатор уязвимости: CVE-2026-70347
BDU:2026-13277

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70347
- https://bdu.fstec.ru/vul/2026-13277

21
9

Краткое описание: Выполнение произвольного кода в Windows Device Health Attestation

Идентификатор уязвимости: CVE-2026-66802
BDU:2026-13280

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.9121
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66802
- https://bdu.fstec.ru/vul/2026-13280

220

Краткое описание: Повышение привилегий в Windows Key Guard

Идентификатор уязвимости: CVE-2026-66799
BDU:2026-13281

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66799
- https://bdu.fstec.ru/vul/2026-13281

221

Краткое описание: Выполнение произвольного кода в Windows iSCSI Target Service

Идентификатор уязвимости: CVE-2026-65791
BDU:2026-13282

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65791
- https://bdu.fstec.ru/vul/2026-13282

Краткое описание: Повышение привилегий в Microsoft Windows Cross Device Service

Идентификатор уязвимости: CVE-2026-66804
BDU:2026-13274

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows 10 22H2: до 10.0.19045.7663
Windows 11 24H2: до 10.0.26100.9106
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

22
2

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-01 / 2026-09-01

Ссылки на источник:

- https://github.com/Rat5ak/CVE-2026-66804-CrossDevice-Service-EoP
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66804
- https://github.com/DavidCarliez/CVE-2026-66804-CrossDevice-LPE
- https://bdu.fstec.ru/vul/2026-13274

223

Краткое описание: Повышение привилегий в CoreDNS

Идентификатор уязвимости: CVE-2026-35579
BDU:2026-13672

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: РЕД ОС: 8.0
Red Hat Advanced Cluster Management for Kubernetes: 2.14
coredns: до 1.14.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://github.com/coredns/coredns/security/advisories/GHSA-vp29-5652-4fw9
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-35579
- https://access.redhat.com/security/cve/cve-2026-35579
- https://bdu.fstec.ru/vul/2026-13672

224

Краткое описание: Выполнение произвольного кода в ROS#

Идентификатор уязвимости: CVE-2026-41551
BDU:2026-13677

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

Уязвимый продукт: ROS#: до 2.2.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-357982.html
- https://github.com/selecthch/CVE-2026-41551
- https://bdu.fstec.ru/vul/2026-13677

225

Краткое описание: Выполнение произвольного кода в elFinder

Идентификатор уязвимости: CVE-2026-81891
BDU:2026-13683

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: elFinder: до 2.1.70

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/Studio-42/elFinder/commit/191372c1bbebbd36fb55af79a84b9984861390ff
- https://github.com/Studio-42/elFinder/commit/dd73e702820c146a192969800ee674ecdb208365
- https://github.com/Studio-42/elFinder/releases/tag/2.1.70
- https://github.com/Studio-42/elFinder/security/advisories/GHSA-gxmj-r5rf-ggwq
- https://bdu.fstec.ru/vul/2026-13683

226

Краткое описание: Получение конфиденциальной информации в elFinder

Идентификатор уязвимости: CVE-2026-81889
BDU:2026-13684

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: elFinder: до 2.1.70

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/Studio-42/elFinder/commit/191372c1bbebbd36fb55af79a84b9984861390ff
- https://github.com/Studio-42/elFinder/commit/6d997386cd0f1abab4706c220b46b0aea0ecff51
- https://github.com/Studio-42/elFinder/releases/tag/2.1.70
- https://github.com/Studio-42/elFinder/security/advisories/GHSA-8x3q-jpjh-qh5c
- https://bdu.fstec.ru/vul/2026-13684

Краткое описание: Отказ в обслуживании в OpenSSL

Идентификатор уязвимости: CVE-2026-63072
BDU:2026-13717

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: OpenSSL: от 4.0.0 до 4.0.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

22
7

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/openssl/openssl/commit/2a3dac874c8057c1f0186849bf1ede1ae7b6b756
- https://github.com/openssl/openssl/commit/87784ad619af36b8807c2044b3940006fccc1e42
- https://github.com/openssl/openssl/commit/9530a5fd1aacaeccdced4478ea2340a480613335
- https://github.com/openssl/openssl/commit/9ec2f6d2ae2bcad907cf7ee38584855bafe4979a
- https://github.com/openssl/openssl/commit/a0c8ec557d9cac078f032d76cdf684fe743eb382
- https://openssl-library.org/news/secadv/20260825.txt
- https://www.strix.ai/cve/CVE-2026-63072
- https://bdu.fstec.ru/vul/2026-13717

228

Краткое описание: Повышение привилегий в Microsoft Exchange Server

Идентификатор уязвимости: CVE-2026-62911
BDU:2026-13469

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: Microsoft Exchange Server Subscription Edition RTM: до 15.02.2562.046
Microsoft Exchange Server 2019 Cumulative Update 15: до 15.02.1748.049
Microsoft Exchange Server 2019 Cumulative Update 14: до 15.02.1544.044
Microsoft Exchange Server 2016 Cumulative Update 23: до 15.01.2507.072

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911
- https://github.com/hypnguyen1209/CVE-2026-62911
- https://gbhackers.com/poc-released-for-microsoft-exchange-cve-2026-62911/
- https://bdu.fstec.ru/vul/2026-13469

229

Краткое описание: Обход безопасности в Python NLTK library

Идентификатор уязвимости: CVE-2026-62388
BDU:2026-13473

Идентификатор программной ошибки: CWE-1005 Отображение и проверка входных данных

Уязвимый продукт: NLTK: до 3.9.4 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/nltk/nltk/security/advisories/GHSA-p3m8-78j2-g5p3
- https://bdu.fstec.ru/vul/2026-13473

230

Краткое описание: Выполнение произвольного кода в SPIP

Идентификатор уязвимости: CVE-2026-77806
BDU:2026-13475

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: SPIP: до 4.4.21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://blog.spip.net/Mise-a-jour-critique-de-securite-sortie-de-SPIP-4-4-21.html
- https://github.com/rapid7/metasploit-framework/pull/21790
- https://github.com/rapid7/metasploit-framework/pull/21790#issuecomment-5368038123
- https://github.com/rapid7/metasploit-framework/pull/21790/commits/b16eca819abb8f1401f21d115e71e3dfc67b847c
- https://github.com/CuteeCat/CVE-2026-77806
- https://bdu.fstec.ru/vul/2026-13475

Краткое описание: Выполнение произвольного кода в Budibase

Идентификатор уязвимости: CVE-2026-54350
BDU:2026-13477

Идентификатор программной ошибки: CWE-1001 Модели программных сбоев (вторичный кластер): использование некорректного API

Уязвимый продукт: Budibase: до 3.39.12 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

231 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/Budibase/budibase/security/advisories/GHSA-8qv3-p479-cj62
- https://bdu.fstec.ru/vul/2026-13477

23
2

Краткое описание: Повышение привилегий в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-62807
BDU:2026-13489

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62807
- https://bdu.fstec.ru/vul/2026-13489

233

Краткое описание: Повышение привилегий в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-62812
BDU:2026-13491

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62812
- https://bdu.fstec.ru/vul/2026-13491

234

Краткое описание: Выполнение произвольного кода в Windows Deployment Services TFTP Server

Идентификатор уязвимости: CVE-2026-62893
BDU:2026-13502

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62893
- https://bdu.fstec.ru/vul/2026-13502

235

Краткое описание: Повышение привилегий в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-62803
BDU:2026-13486

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9121
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9121
Windows Server 2019 (Server Core installation): до 10.0.17763.9121
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62803
- https://bdu.fstec.ru/vul/2026-13486

236

Краткое описание: Отказ в обслуживании в Python NLTK library

Идентификатор уязвимости: CVE-2026-66393
BDU:2026-13471

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: NLTK: до 3.9.3 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/nltk/nltk/security/advisories/GHSA-rf74-v2fm-23pw
- https://bdu.fstec.ru/vul/2026-13471

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-80724
BDU:2026-13721

Идентификатор программной ошибки: CWE-279 Некорректное назначение разрешений при выполнении

Уязвимый продукт: Linux: от 7.2 до 7.2.1
Ubuntu: 26.04 LTS

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

237

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026082811-CVE-2026-80724-bc86@gregkh/
- https://git.kernel.org/stable/c/5b4f2bec7bea6c04084d720d731bedee7caf878d
- https://git.kernel.org/stable/c/2496e141827102d6af512950057d402a2cfb2bfc
- https://git.kernel.org/stable/c/2e596e7814ba38cdc129991058b6c254ed37cb11
- https://git.kernel.org/stable/c/a5edadbae57e2298a56cf7a4e774a027905a331f
- https://access.redhat.com/security/cve/cve-2026-80724
- https://ubuntu.com/security/CVE-2026-80724
- https://github.com/suruurism/cve-writeups-and-pocs
- https://bdu.fstec.ru/vul/2026-13721

238

Краткое описание: Потеря целостности в XMLDOM

Идентификатор уязвимости: CVE-2026-83618
BDU:2026-13729

Идентификатор программной ошибки: CWE-625 Некорректное ограничение регулярных выражений

Уязвимый продукт: XMLDOM: от 0.9.10 до 0.9.12

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/xmldom/xmldom/commit/7b2ec67e1750daadd0bb06c92e875e726544a362
- https://github.com/xmldom/xmldom/pull/1071
- https://github.com/xmldom/xmldom/releases/tag/0.9.12
- https://github.com/xmldom/xmldom/security/advisories/GHSA-vr34-hp96-76pp
- https://bdu.fstec.ru/vul/2026-13729

239

Краткое описание: Отказ в обслуживании в XMLDOM

Идентификатор уязвимости: CVE-2026-83619
BDU:2026-13730

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: XMLDOM: от 0.7.0 до 0.8.15

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/xmldom/xmldom/commit/3abb0934f5a8a84d83a1f9cde0f2bd04c08b2a09
- https://github.com/xmldom/xmldom/security/advisories/GHSA-x4fp-j954-r2f4
- https://github.com/xmldom/xmldom/releases/tag/0.8.15
- https://github.com/xmldom/xmldom/pull/1072
- https://bdu.fstec.ru/vul/2026-13730

240

Краткое описание: Обход безопасности в XMLDOM

Идентификатор уязвимости: CVE-2026-83617
BDU:2026-13731

Идентификатор программной ошибки: CWE-625 Некорректное ограничение регулярных выражений

Уязвимый продукт: XMLDOM: до 0.9.12

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/xmldom/xmldom/security/advisories/GHSA-jxjr-3g7g-3944
- https://github.com/xmldom/xmldom/commit/7b2ec67e1750daadd0bb06c92e875e726544a362
- https://github.com/xmldom/xmldom/pull/1071
- https://github.com/xmldom/xmldom/releases/tag/0.9.12
- https://bdu.fstec.ru/vul/2026-13731

241

Краткое описание: Отказ в обслуживании в XMLDOM

Идентификатор уязвимости: CVE-2026-83612
BDU:2026-13732

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: XMLDOM: от 0.9.0-beta.1 до 0.9.12

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/xmldom/xmldom/security/advisories/GHSA-6mj3-qw4j-hgrw
- https://github.com/xmldom/xmldom/releases/tag/0.9.12
- https://github.com/xmldom/xmldom/pull/1071
- https://github.com/xmldom/xmldom/commit/7ced40c06c28d151e996a97045018c3559ae4707
- https://bdu.fstec.ru/vul/2026-13732

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-63520
BDU:2026-13743

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20522
Microsoft SharePoint Enterprise Server 2016: до 16.0.5565.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20198

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

24
2

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-03 / 2026-09-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63520
- https://www.linkedin.com/posts/ishaank1_cybersecurity-microsoftsharepoint-cve202663520-activity-7493602553432006657-Oabx
- https://www.bleepingcomputer.com/news/security/hackers-target-microsoft-sharepoint-rce-chain-with-poc-exploit/
- https://www.vulncheck.com/blog/cve-2026-63520-sharepoint-unsafe-type-rce
- https://bdu.fstec.ru/vul/2026-13743

243

Краткое описание: Обход безопасности в Traefik

Идентификатор уязвимости: CVE-2026-48020
BDU:2026-13744

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Traefik: от 3.7.0 до 3.7.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-03 / 2026-09-03

Ссылки на источник:

- https://github.com/traefik/traefik/releases/tag/v2.11.48
- https://github.com/traefik/traefik/releases/tag/v3.6.19
- https://github.com/traefik/traefik/releases/tag/v3.7.3
- https://github.com/traefik/traefik/security/advisories/GHSA-xf64-8mw2-4gr2
- https://advisories.gitlab.com/golang/github.com/traefik/traefik/v2/CVE-2026-48020/
- https://bdu.fstec.ru/vul/2026-13744

244

Краткое описание: Межсайтовый скриптинг в LibreNMS

Идентификатор уязвимости: CVE-2026-84189
BDU:2026-13728

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: LibreNMS: до 26.7.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-02 / 2026-09-02

Ссылки на источник:

- https://github.com/librenms/librenms/security/advisories/GHSA-7gww-x7fh-jf9j
- https://feedly.com/cve/CVE-2026-84189
- https://bdu.fstec.ru/vul/2026-13728

245

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53202
BDU:2026-14034

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.8 до 6.12.93 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53202
- https://git.kernel.org/stable/c/4788556d4dd9d717037e385de178974e9649231d
- https://git.kernel.org/stable/c/45cb105b8642c65e9be286f7058e92314efe7ea3
- https://git.kernel.org/stable/c/2821bf2b79e47f87e1dbdd9d25c78240965a97d6
- https://git.kernel.org/linus/d9faef564438d1e4579c692c046603e7ada7bdf4
- https://security-tracker.debian.org/tracker/CVE-2026-53202
- https://access.redhat.com/security/cve/CVE-2026-53202
- https://ubuntu.com/security/CVE-2026-53202

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53202
- https://bdu.fstec.ru/vul/2026-14034

246

Краткое описание: Чтение локальных файлов в Open edX Platform

Идентификатор уязвимости: CVE-2026-53635
BDU:2026-14040

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Open edX Platform: ulmo

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://github.com/openedx/openedx-platform/security/advisories/GHSA-rqq6-w4pv-7pjv
- https://bdu.fstec.ru/vul/2026-14040

247

Краткое описание: Обход безопасности в Open edX Platform

Идентификатор уязвимости: CVE-2026-53636
BDU:2026-14041

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: Open edX Platform: ulmo

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://github.com/openedx/openedx-platform/security/advisories/GHSA-6gm5-c49g-p3h9
- https://bdu.fstec.ru/vul/2026-14041

248

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53221
BDU:2026-14047

Идентификатор программной ошибки: CWE-1076 Несоответствие принятым стандартам

Уязвимый продукт: Linux: от 3.19 до 5.10.258 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53221
- https://git.kernel.org/stable/c/c327fa4fca31415431202e063767a7ae342e19c6
- https://git.kernel.org/stable/c/fc657ac0767c49839b3ef0b08dc0953ca30883f8
- https://git.kernel.org/stable/c/47fb3c2b4203556308e64354b3e78f2ce221d646
- https://git.kernel.org/stable/c/f513f308cc4bdb4530d033431592ffbc29b7fca1
- https://git.kernel.org/stable/c/90fd4513315ca07da99cfd8549d3e553a7160f0d
- https://git.kernel.org/stable/c/2abfb19bbb81958714ad1d43ebeb65b30394184b
- https://git.kernel.org/stable/c/2fc7bc087cc7085368263d9d37bfe9a0bddd6a2d

- https://git.kernel.org/linus/a5c0359f5cbc51a2e2b114d6041e0f3c73f903e9
- https://security-tracker.debian.org/tracker/CVE-2026-53221
- https://access.redhat.com/security/cve/CVE-2026-53221
- https://ubuntu.com/security/CVE-2026-53221
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53221
- https://bdu.fstec.ru/vul/2026-14047

249

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-85046
BDU:2026-14048

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: до 152.0.7977.82

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://securityonline.info/chrome-zero-day-vulnerability/
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://github.com/Serotav/Writeups/blob/77556c57999805fa7815a114da51d91cf24fbea9/v8/When_Sorting_Leads_To_Confusion.md
- https://serotav.github.io/Writeups/v8/when-sorting-leads-to-confusion/
- https://bdu.fstec.ru/vul/2026-14048

250

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53226
BDU:2026-14050

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 5.15 до 6.18.35 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53226
- https://git.kernel.org/stable/c/bace7b99bfa555fe833aee8827b8004c43666d02
- https://git.kernel.org/stable/c/1f34ea5f6114011092d9a5c8b901ad6741144a1d
- https://git.kernel.org/linus/1c1e0fc88d6ef65bf15d517853251f75ab9d18c3
- https://security-tracker.debian.org/tracker/CVE-2026-53226
- https://ubuntu.com/security/CVE-2026-53226
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53226
- https://bdu.fstec.ru/vul/2026-14050

251

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53228
BDU:2026-14052

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 3.18 до 5.10.258 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53228
- https://git.kernel.org/stable/c/fddd41445a0537b093e6b3f6232c9933cad1e48b
- https://git.kernel.org/stable/c/1132e5edc2866c3530be17622153a597095f0e43
- https://git.kernel.org/stable/c/9c67b44edb3598d234efae6e44649eb993c03da5
- https://git.kernel.org/stable/c/0bfa7bba1f41aaf5f0604dc712bb4701493e3aa0
- https://git.kernel.org/stable/c/59f80c919713250fe5d25a4d9aea4e49580fa1d4
- https://git.kernel.org/stable/c/2fa49b2715e1bad12ce3b0fa64e234d9582c8193
- https://git.kernel.org/stable/c/cb658c2f5f7977c2a1c77c9f239f4bc8196edb5c

- https://git.kernel.org/linus/f0e42f0c4337b1f220de1ddd63f47197c7dee4de
- https://security-tracker.debian.org/tracker/CVE-2026-53228
- https://access.redhat.com/security/cve/CVE-2026-53228
- https://ubuntu.com/security/CVE-2026-53228
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53228
- https://bdu.fstec.ru/vul/2026-14052

252

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53240
BDU:2026-14058

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.14 до 6.18.35 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53240
- https://git.kernel.org/stable/c/8d9a79fbf5172d9c4c0146057af2360913265a11
- https://git.kernel.org/stable/c/ff2ee35b6ce5fa8a8e24ea50b15733d5c8780198
- https://git.kernel.org/linus/eb48730bb827d1550401a5d391903f9d90b493c8
- https://ubuntu.com/security/CVE-2026-53240
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53240
- https://bdu.fstec.ru/vul/2026-14058

253

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53246
BDU:2026-14061

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.12 до 6.18.35 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53246
- https://git.kernel.org/stable/c/cc272185c9a9a4b7febc2de52eeaa3d00f19091e
- https://git.kernel.org/stable/c/edccbf3d63b0a3362bc916ea72edacc1e1ca456a
- https://git.kernel.org/linus/0861615c28de668669d748ef4eb913ea9262d13b
- https://security-tracker.debian.org/tracker/CVE-2026-53246
- https://access.redhat.com/security/cve/CVE-2026-53246
- https://ubuntu.com/security/CVE-2026-53246
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53246

- https://bdu.fstec.ru/vul/2026-14061

254

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53225
BDU:2026-14049

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 2.6.25 до 5.10.258 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53225
- https://git.kernel.org/stable/c/446e0ecd845abc394b24ae2030a883572bec9d16
- https://git.kernel.org/stable/c/928dd94db23e8ba340f83d68f7f24d831b7a4426
- https://git.kernel.org/stable/c/d796cfd06074b579d265b28401306cadd30db945
- https://git.kernel.org/stable/c/8ce96f1182644079249a24ac7e2ffc32e0301a46
- https://git.kernel.org/stable/c/d6bd0bb7697ea8c0387b0d9d973453f479017b23
- https://git.kernel.org/stable/c/f76a8b323e28e0951f979dbef20a7496383c47df
- https://git.kernel.org/stable/c/8e86817b8af4d552f3c6fe04ca52bb0c8c57411d

- https://git.kernel.org/linus/f8373d7090b745728de66308deeecc67e8d319ce
- https://security-tracker.debian.org/tracker/CVE-2026-53225
- https://access.redhat.com/security/cve/CVE-2026-53225
- https://ubuntu.com/security/CVE-2026-53225
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53225
- https://bdu.fstec.ru/vul/2026-14049

255

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53176
BDU:2026-14020

Идентификатор программной ошибки: CWE-839 Отсутствует проверка на соответствие минимальному значению диапазона

Уязвимый продукт: Linux: от 3.10 до 5.10.258 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53176
- https://git.kernel.org/stable/c/75ee6e4aa096aa9e7b2dd5c8ff98356e30aceefb
- https://git.kernel.org/stable/c/e8a013c0c3ca2f6708341a56612a3f6d6921620a
- https://git.kernel.org/stable/c/bd22740d7f14cb1c0289444cfd2c8d2938667c1d
- https://git.kernel.org/stable/c/c1234229399f4af12c553b1b0ffd978eeba65548
- https://git.kernel.org/stable/c/c5584e089b5af7b3bf8bd5e8ca0560cbf32b0a47
- https://git.kernel.org/stable/c/df422fd273c96c2ee5beb80fc21adc8c70c29260
- https://git.kernel.org/stable/c/1ca40b243277c9e88be5e00bd3e083f71aefb93e

- https://git.kernel.org/linus/29e7b925ae6df64894e82ab6419994dc25580a8a
- https://security-tracker.debian.org/tracker/CVE-2026-53176
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53176
- https://access.redhat.com/security/cve/CVE-2026-53176
- https://ubuntu.com/security/CVE-2026-53176
- https://bdu.fstec.ru/vul/2026-14020

256

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53178
BDU:2026-14021

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Linux: от 5.15 до 7.0.12 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53178
- https://git.kernel.org/stable/c/542d65a6dbd9733baab96313c9fe76a76e93f484
- https://git.kernel.org/linus/88e994c57a79f62d5338231d8d37ee8dd98baffe
- https://security-tracker.debian.org/tracker/CVE-2026-53178
- https://ubuntu.com/security/CVE-2026-53178
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53178
- https://bdu.fstec.ru/vul/2026-14021

257

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53175
BDU:2026-14019

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.18.3 до 6.18.35 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53175
- https://git.kernel.org/stable/c/0e823ca0e7391630784ae7dd0981b7ad170a93d9
- https://git.kernel.org/stable/c/c22599cc90e1cd5f8129c8670bd68a02ff7177b4
- https://git.kernel.org/stable/c/89b909e9704587bfecc1aab1d37e98faee03b9f9
- https://git.kernel.org/stable/c/010c3313a4d178dc2d3ce958d2e5cb055e2864c1
- https://git.kernel.org/linus/32594b09854970d7ba83eb2dc8c69a2edd158c8e
- https://ubuntu.com/security/CVE-2026-53175
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53175
- https://bdu.fstec.ru/vul/2026-14019

25
8

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53170
BDU:2026-14016

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 6.19 до 7.0.12 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 10

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53170
- https://git.kernel.org/stable/c/fb25c76a820ca8a547aa478bfb503da0a11494ab
- https://git.kernel.org/linus/d9d021218162b6c4fe0bdf42b2b340f1aae23a12
- https://ubuntu.com/security/CVE-2026-53170
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53170
- https://bdu.fstec.ru/vul/2026-14016

259

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53159
BDU:2026-14013

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Linux: от 5.1.6 до 5.15.209 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53159
- https://git.kernel.org/stable/c/2d0f47e27c1fa718b29c69aa7c96a2c5161bc2c2
- https://git.kernel.org/stable/c/708c17b52c60fe7a57e73b495bdee50f58feb48c
- https://git.kernel.org/stable/c/d3e26df2e8eb361e6bef096b2fd565476a1f14c4
- https://git.kernel.org/stable/c/e69e306a4cccb40a73511350cb280825a556ce3c
- https://git.kernel.org/stable/c/53e06f8a3c2b085c31bf1284e2ebcb8036e99625
- https://git.kernel.org/stable/c/7ba7b30ddb04646d4d638f4d8c4718a304bbbddd
- https://git.kernel.org/linus/464c6ad2aa16e1e1df9d559289199356493d1e00
- https://security-tracker.debian.org/tracker/CVE-2026-53159

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53159
- https://ubuntu.com/security/CVE-2026-53159
- https://bdu.fstec.ru/vul/2026-14013

260

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53260
BDU:2026-14066

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.12 до 7.0.12 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53260
- https://git.kernel.org/stable/c/b183215ff714efb747d9d5a429322ba6404b5401
- https://git.kernel.org/linus/e10902df24488ca722303133acfc82490f7d59ad
- https://security-tracker.debian.org/tracker/CVE-2026-53260
- https://access.redhat.com/security/cve/CVE-2026-53260
- https://ubuntu.com/security/CVE-2026-53260
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53260
- https://bdu.fstec.ru/vul/2026-14066

261

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53266
BDU:2026-14070

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Linux: от 5.9.2 до 5.10.258 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53266
- https://git.kernel.org/stable/c/bf84ad7c7a9ede46e31afaa41a1ba06a159e8c87
- https://git.kernel.org/stable/c/76280b78cc9f23bdc6438e10ad6dff148ef8375b
- https://git.kernel.org/stable/c/b7e91939ba9be805a62a257fa4e227dffbb88fa0
- https://git.kernel.org/stable/c/afd64b59c3de9bbbdd3759e834fdc55cda716e0b
- https://git.kernel.org/stable/c/153ea96c806aea395daba907a4f88480b6ad5093
- https://git.kernel.org/stable/c/b18675263db1147c8e1cab625400c13a0d87bd2d
- https://git.kernel.org/stable/c/c9b5ff59feffb92a147a84a5aa28acd2cb8ff4c5

- https://git.kernel.org/linus/67ba971ae02514d85818fe0c32549ab4bfa3bf49
- https://security-tracker.debian.org/tracker/CVE-2026-53266
- https://access.redhat.com/security/cve/CVE-2026-53266
- https://ubuntu.com/security/CVE-2026-53266
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53266
- https://bdu.fstec.ru/vul/2026-14070

262

Краткое описание: Обход безопасности в FortiWeb

Идентификатор уязвимости: CVE-2026-26035
BDU:2026-14146

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FortiWeb: от 7.0.0 до 7.0.12 включительно

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-158
- https://bdu.fstec.ru/vul/2026-14146

Краткое описание: Повышение привилегий в Atlassian Confluence

Идентификатор уязвимости: BDU:2026-14138

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Confluence Server: от 8.5.0 до 8.5.2
Jira Data Center: от 8.5.0 до 8.5.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

263

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://github.com/Chocapikk/CVE-2023-22515
- https://github.com/vulhub/vulhub/tree/master/confluence/CVE-2023-22515
- https://www.kaspersky.ru/blog/confluence-data-center-server-vulnerability/36447/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2023-22515
- https://www.rapid7.com/blog/post/ra-cve-2023-22515-analysis/
- https://confluence.atlassian.com/security/cve-2023-22515-broken-access-control-vulnerability-in-confluence-data-center-and-server-1295682276.html
- https://bdu.fstec.ru/vul/2026-14138