НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-09-17.1 | 17 сентября 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-83609	XMLDOM	Сетевой	SB	2026-09-02	✓
2	Высокая	CVE-2026-83606	XMLDOM	Сетевой	DoS	2026-09-02	✓
3	Высокая	CVE-2026-84304	gRPC-Go	Сетевой	DoS	2026-09-03	✓
4	Критическая	CVE-2026-84372	Predis	Сетевой	DoS	2026-09-04	✓
5	Высокая	CVE-2026-8609	Grafana	Сетевой	DoS	2026-08-31	✓
6	Критическая	CVE-2026-7813	pgAdmin 4	Сетевой	PE	2026-08-31	✓
7	Высокая	CVE-2026-6914	MongoDB Server	Сетевой	ACE	2026-08-28	✓
8	Высокая	CVE-2026-57108	.NET	Сетевой	DoS	2026-08-27	✓
9	Высокая	CVE-2026-53268	Linux	Сетевой	DoS	2026-08-28	✓
10	Высокая	CVE-2026-53277	Linux	Локальный	ACE	2026-08-28	✓
11	Высокая	CVE-2026-53281	Linux	Локальный	ACE	2026-08-28	✓
12	Высокая	CVE-2026-53282	Linux	Смежная сеть	ACE	2026-08-28	✓
13	Высокая	CVE-2026-53290	Linux	Локальный	ACE	2026-08-27	✓

14	Высокая	CVE-2026-53296	Linux	Локальный	ACE	2026-08-31	✓
15	Высокая	CVE-2026-53262	Linux	Локальный	ACE	2026-08-27	✓
16	Высокая	CVE-2026-53145	Linux	Локальный	ACE	2026-08-27	✓
17	Высокая	CVE-2026-33382	Grafana	Сетевой	DoS	2026-08-31	✓
18	Высокая	CVE-2026-40684	exim	Сетевой	OSI	2026-08-24	✓
19	Критическая	CVE-2026-40685	exim	Сетевой	OSI	2026-08-24	✓
20	Критическая	CVE-2026-56372	ImageMagick	Сетевой	ACE	2026-08-25	✓
21	Высокая	CVE-2026-53137	Linux	Смежная сеть	ACE	2026-08-28	✓
22	Высокая	CVE-2026-53148	Linux	Локальный	ACE	2026-08-28	✓
23	Высокая	CVE-2026-53109	Linux	Локальный	ACE	2026-08-28	✓
24	Высокая	CVE-2026-52922	Linux	Сетевой	DoS	2026-08-27	✓
25	Критическая	CVE-2026-52924	Linux	Сетевой	ACE	2026-08-28	✓
26	Высокая	CVE-2026-52927	Linux	Локальный	ACE	2026-08-27	✓
27	Высокая	CVE-2026-52929	Linux	Сетевой	DoS	2026-08-27	✓
28	Высокая	CVE-2026-52932	Linux	Сетевой	DoS	2026-08-27	✓

29	Высокая	CVE-2026-52935	Linux	Локальный	ACE	2026-08-27	✓
30	Высокая	CVE-2026-53135	Linux	Смежная сеть	ACE	2026-08-28	✓
31	Высокая	CVE-2026-52951	Linux	Локальный	ACE	2026-08-27	✓
32	Высокая	CVE-2026-52952	Linux	Локальный	ACE	2026-08-28	✓
33	Высокая	CVE-2026-52954	Linux	Сетевой	DoS	2026-08-27	✓
34	Критическая	CVE-2026-52955	Linux	Сетевой	ACE	2026-08-28	✓
35	Высокая	CVE-2026-52956	Linux	Сетевой	DoS	2026-08-27	✓
36	Высокая	CVE-2026-52957	Linux	Сетевой	DoS	2026-08-27	✓
37	Высокая	CVE-2026-52950	Linux	Локальный	ACE	2026-08-27	✓
38	Критическая	CVE-2026-52958	Linux	Сетевой	DoS	2026-08-28	✓
39	Высокая	CVE-2026-52920	Linux	Сетевой	ACE	2026-08-28	✓
40	Высокая	CVE-2026-46332	Linux	Смежная сеть	ACE	2026-08-27	✓
41	Высокая	CVE-2026-63828	Linux	Локальный	CI	2026-09-04	✓
42	Критическая	CVE-2026-53363	Linux	Сетевой	ACE	2026-08-31	✓
43	Критическая	CVE-2026-53355	Linux	Сетевой	ACE	2026-08-31	✓

44	Высокая	CVE-2026-53343	Linux	Смежная сеть	ACE	2026-08-31	✓
45	Высокая	CVE-2026-53329	Linux	Смежная сеть	ACE	2026-08-31	✓
46	Высокая	CVE-2026-53322	Linux	Локальный	ACE	2026-08-28	✓
47	Высокая	CVE-2026-52909	Linux	Локальный	ACE	2026-08-28	✓
48	Высокая	CVE-2026-46288	Linux	Локальный	ACE	2026-08-25	✓
49	Высокая	CVE-2026-46301	Linux	Смежная сеть	ACE	2026-08-25	✓
50	Высокая	CVE-2026-46304	Linux	Сетевой	DoS	2026-08-25	✓
51	Высокая	CVE-2026-46308	Linux	Смежная сеть	ACE	2026-08-25	✓
52	Высокая	CVE-2026-46311	Linux	Локальный	ACE	2026-08-25	✓
53	Высокая	CVE-2026-46317	Linux	Локальный	ACE	2026-08-27	✓
54	Высокая	CVE-2026-46319	Linux	Локальный	ACE	2026-08-27	✓
55	Высокая	CVE-2026-46290	Linux	Смежная сеть	ACE	2026-08-25	✓
56	Высокая	CVE-2026-52959	Linux	Локальный	ACE	2026-08-27	✓
57	Высокая	CVE-2026-52947	Linux	Локальный	ACE	2026-08-27	✓

58	Высокая	CVE-2026-52973	Linux	Локальный	ACE	2026-08-27	✓
59	Высокая	CVE-2026-53094	Linux	Локальный	ACE	2026-08-27	✓
60	Высокая	CVE-2026-53092	Linux	Локальный	ACE	2026-08-28	✓
61	Высокая	CVE-2026-53091	Linux	Локальный	DoS	2026-08-28	✓
62	Высокая	CVE-2026-53090	Linux	Локальный	ACE	2026-08-27	✓
63	Высокая	CVE-2026-53085	Linux	Локальный	ACE	2026-08-27	✓
64	Высокая	CVE-2026-52969	Linux	Локальный	ACE	2026-08-28	✓
65	Высокая	CVE-2026-53078	Linux	Локальный	ACE	2026-08-27	✓
66	Высокая	CVE-2026-53071	Linux	Смежная сеть	ACE	2026-08-27	✓
67	Высокая	CVE-2026-53069	Linux	Сетевой	DoS	2026-08-27	✓
68	Высокая	CVE-2026-53067	Linux	Локальный	ACE	2026-08-28	✓
69	Критическая	CVE-2026-53055	Linux	Сетевой	ACE	2026-08-28	✓
70	Высокая	CVE-2026-53054	Linux	Локальный	ACE	2026-08-27	✓
71	Критическая	CVE-2026-53045	Linux	Сетевой	ACE	2026-08-28	✓
72	Высокая	CVE-2026-53033	Linux	Локальный	ACE	2026-08-27	✓

73	Высокая	CVE-2026-53031	Linux	Локальный	ACE	2026-08-27	✓
74	Высокая	CVE-2026-53081	Linux	Локальный	ACE	2026-08-27	✓
75	Высокая	CVE-2026-53016	Linux	Локальный	ACE	2026-08-27	✓
76	Высокая	CVE-2026-52976	Linux	Локальный	ACE	2026-08-27	✓
77	Высокая	CVE-2026-53020	Linux	Локальный	ACE	2026-08-27	✓
78	Высокая	CVE-2026-52981	Linux	Сетевой	DoS	2026-08-27	✓
79	Критическая	CVE-2026-52989	Linux	Сетевой	ACE	2026-08-27	✓
80	Высокая	CVE-2026-52991	Linux	Локальный	ACE	2026-08-27	✓
81	Критическая	CVE-2026-52993	Linux	Сетевой	ACE	2026-08-28	✓
82	Высокая	CVE-2026-52998	Linux	Сетевой	DoS	2026-08-27	✓
83	Высокая	CVE-2026-52987	Linux	Локальный	ACE	2026-08-27	✓
84	Высокая	CVE-2026-53000	Linux	Локальный	ACE	2026-08-27	✓
85	Критическая	CVE-2026-53002	Linux	Сетевой	ACE	2026-08-28	✓
86	Высокая	CVE-2026-53004	Linux	Локальный	ACE	2026-08-28	✓
87	Критическая	CVE-2026-53006	Linux	Сетевой	ACE	2026-08-27	✓

88	Высокая	CVE-2026-53009	Linux	Локальный	ACE	2026-08-28	✓
89	Высокая	CVE-2026-53011	Linux	Локальный	ACE	2026-08-27	✓
90	Критическая	CVE-2026-52999	Linux	Сетевой	DoS	2026-08-28	✓
91	Высокая	CVE-2026-45906	Linux	Локальный	ACE	2026-08-25	✓
92	Критическая	CVE-2026-19490	NetScaler Gateway	Сетевой	ACE	2026-09-04	✓
93	Высокая	CVE-2026-84361	Composer	Сетевой	ACE	2026-09-04	✓
94	Критическая	CVE-2026-12841	Python NLTK library	Сетевой	PE	2026-09-04	✓
95	Критическая	CVE-2026-46039	Linux	Сетевой	ACE	2026-08-25	✓
96	Высокая	CVE-2026-46075	Linux	Локальный	ACE	2026-08-25	✓
97	Высокая	CVE-2026-46205	Linux	Локальный	ACE	2026-08-25	✓
98	Критическая	CVE-2026-46115	Linux	Сетевой	ACE	2026-08-25	✓
99	Высокая	CVE-2026-46120	Linux	Локальный	ACE	2026-08-25	✓
100	Высокая	CVE-2026-45929	Linux	Локальный	ACE	2026-08-25	✓
101	Высокая	CVE-2026-46053	Linux	Локальный	ACE	2026-08-25	✓
102	Высокая	CVE-2026-46209	Linux	Локальный	ACE	2026-08-25	✓

103	Высокая	CVE-2026-46201	Linux	Локальный	ACE	2026-08-25	✓
104	Высокая	CVE-2026-46173	Linux	Локальный	ACE	2026-08-25	✓
105	Высокая	CVE-2026-46081	Linux	Локальный	ACE	2026-08-25	✓
106	Высокая	CVE-2026-46241	Linux	Смежная сеть	ACE	2026-08-25	✓
107	Критическая	CVE-2026-25786	SIMATIC S7 PLC	Сетевой	XSS\CSS	2026-05-13	✓
108	Высокая	CVE-2026-27662	SIMATIC HMI Unified Comfort	Локальный	PE	2026-05-13	✓
109	Высокая	CVE-2026-76642	Util-linux	Локальный	PE	2026-09-07	✓
110	Критическая	CVE-2026-52490	LibTIFF	Сетевой	ACE	2026-09-07	✓
111	Высокая	CVE-2026-70465	FortiClient Windows	Сетевой	ACE	2026-08-26	✓
112	Высокая	CVE-2026-0292	Prisma Access Agent	Локальный	SB	2026-08-21	✓
113	Высокая	CVE-2026-0294	Prisma Access Agent	Локальный	PE	2026-08-24	✓
114	Высокая	CVE-2026-0297	GlobalProtect App	Сетевой	ACE	2026-08-24	✓
115	Высокая	CVE-2026-0299	GlobalProtect App	Локальный	PE	2026-08-24	✓
116	Высокая	CVE-2026-0301	PAN-OS	Сетевой	OSI	2026-08-24	✓
117	Высокая	CVE-2026-11917	ThinManager	Сетевой	OAF	2026-07-16	✓

118	Критическая	CVE-2026-0291	Prisma Access Agent	Сетевой	DoS	2026-08-21	✓
119	Высокая	CVE-2026-85591	phpMyFAQ	Сетевой	OSI	2026-09-07	✓
120	Высокая	CVE-2026-84115	Cleo Harmony	Сетевой	PE	2026-09-07	✓
121	Высокая	CVE-2026-75438	Open5GS	Сетевой	DoS	2026-09-08	✓
122	Высокая	CVE-2026-64563	Linux	Локальный	DoS	2026-09-08	✓
123	Высокая	CVE-2026-53264	Linux	Локальный	DoS	2026-09-08	✓
124	Высокая	CVE-2026-64076	Linux	Локальный	ACE	2026-09-08	✓
125	Высокая	CVE-2026-63911	Linux	Локальный	ACE	2026-09-08	✓
126	Высокая	CVE-2026-63875	Linux	Локальный	ACE	2026-09-08	✓
127	Высокая	CVE-2026-63879	Linux	Локальный	ACE	2026-09-08	✓
128	Критическая	CVE-2026-64046	Linux	Сетевой	ACE	2026-09-08	✓
129	Критическая	CVE-2026-63888	Linux	Сетевой	ACE	2026-09-08	✓
130	Критическая	CVE-2026-63886	Linux	Сетевой	ACE	2026-09-08	✓
131	Критическая	CVE-2026-64150	Linux	Сетевой	ACE	2026-09-08	✓
132	Критическая	CVE-2026-64028	Linux	Сетевой	ACE	2026-09-08	✓

133	Критическая	CVE-2026-63922	Linux	Сетевой	ACE	2026-09-08	✓
134	Критическая	CVE-2026-28316	SolarWinds Serv-U	Сетевой	PE	2026-08-03	✓
135	Критическая	CVE-2026-28314	SolarWinds Serv-U	Сетевой	PE	2026-08-03	✓
136	Критическая	CVE-2026-28321	SolarWinds Serv-U	Сетевой	PE	2026-08-03	✓
137	Критическая	CVE-2026-28313	SolarWinds Serv-U	Сетевой	PE	2026-08-03	✓
138	Критическая	CVE-2026-63924	Linux	Сетевой	ACE	2026-09-08	✓
139	Высокая	CVE-2026-64104	Linux	Локальный	ACE	2026-09-08	✓
140	Высокая	CVE-2026-63906	Linux	Локальный	ACE	2026-09-08	✓
141	Высокая	CVE-2026-64081	Linux	Локальный	ACE	2026-09-08	✓
142	Критическая	CVE-2026-28317	SolarWinds Serv-U	Сетевой	PE	2026-08-03	✓
143	Критическая	CVE-2026-28312	SolarWinds Serv-U	Сетевой	ACE	2026-07-23	✓
144	Высокая	CVE-2026-64151	Linux	Локальный	CI	2026-09-08	✓
145	Критическая	CVE-2026-28304	SolarWinds Serv-U	Сетевой	ACE	2026-07-23	✓
146	Высокая	CVE-2026-53380	Linux	Локальный	ACE	2026-09-08	✓
147	Критическая	CVE-2026-53384	Linux	Сетевой	ACE	2026-09-08	✓

148	Высокая	CVE-2026-53389	Linux	Локальный	ACE	2026-09-08	✓
149	Критическая	CVE-2026-83941	Microsoft Entra ID	Сетевой	PE	2026-09-07	✓
150	Высокая	CVE-2026-63881	Linux	Локальный	ACE	2026-09-08	✓
151	Высокая	CVE-2026-65818	Microsoft Power Automate	Сетевой	PE	2026-09-08	✓
152	Критическая	CVE-2026-62916	Microsoft Entra ID	Сетевой	PE	2026-09-08	✓
153	Критическая	CVE-2026-80098	Microsoft Copilot Studio	Сетевой	PE	2026-09-07	✓
154	Критическая	CVE-2026-83711	Microsoft Azure Active Directory B2C	Сетевой	PE	2026-09-07	✓
155	Критическая	CVE-2026-28302	SolarWinds Serv-U	Сетевой	ACE	2026-07-23	✓
156	Высокая	CVE-2026-64071	Linux	Локальный	ACE	2026-09-08	✓
157	Высокая	CVE-2026-63794	Linux	Локальный	ACE	2026-09-08	✓
158	Высокая	CVE-2026-64191	Linux	Локальный	ACE	2026-09-08	✓
159	Высокая	CVE-2026-64048	Linux	Сетевой	DoS	2026-09-08	✓
160	Высокая	CVE-2026-63983	Linux	Сетевой	DoS	2026-09-08	✓
161	Высокая	CVE-2026-63969	Linux	Сетевой	DoS	2026-09-08	✓
162	Высокая	CVE-2026-64094	Linux	Сетевой	DoS	2026-09-08	✓

163	Высокая	CVE-2026-63869	Linux	Смежная сеть	ACE	2026-09-08	✓
164	Высокая	CVE-2026-63933	Linux	Локальный	ACE	2026-09-08	✓
165	Высокая	CVE-2026-64050	Linux	Локальный	ACE	2026-09-08	✓
166	Высокая	CVE-2026-64004	Linux	Локальный	ACE	2026-09-08	✓
167	Высокая	CVE-2026-63927	Linux	Локальный	ACE	2026-09-08	✓
168	Высокая	CVE-2026-63910	Linux	Локальный	ACE	2026-09-08	✓
169	Высокая	CVE-2026-63855	Linux	Локальный	ACE	2026-09-08	✓
170	Критическая	CVE-2026-28310	SolarWinds Serv-U	Сетевой	PE	2026-07-23	✓
171	Высокая	CVE-2026-64051	Linux	Локальный	ACE	2026-09-08	✓
172	Критическая	CVE-2026-28308	SolarWinds Serv-U	Сетевой	ACE	2026-07-23	✓
173	Критическая	CVE-2026-63962	Linux	Сетевой	ACE	2026-09-08	✓
174	Критическая	CVE-2026-64106	Linux	Локальный	DoS	2026-09-08	✓
175	Высокая	CVE-2026-63959	Linux	Локальный	ACE	2026-09-08	✓
176	Высокая	CVE-2026-64030	Linux	Смежная сеть	ACE	2026-09-08	✓
177	Высокая	CVE-2026-53374	Linux	Локальный	ACE	2026-09-08	✓

178	Высокая	CVE-2026-53375	Linux	Локальный	ACE	2026-09-08	✓
179	Высокая	CVE-2026-64117	Linux	Смежная сеть	ACE	2026-09-08	✓
180	Высокая	CVE-2026-64124	Linux	Локальный	ACE	2026-09-08	✓
181	Высокая	CVE-2026-64153	Linux	Локальный	ACE	2026-09-08	✓
182	Высокая	CVE-2026-63863	Linux	Локальный	ACE	2026-09-08	✓
183	Критическая	CVE-2026-63938	Linux	Локальный	ACE	2026-09-08	✓
184	Высокая	CVE-2026-63865	Linux	Локальный	ACE	2026-09-08	✓
185	Высокая	CVE-2026-63921	Linux	Локальный	ACE	2026-09-08	✓
186	Высокая	CVE-2026-64093	Linux	Смежная сеть	ACE	2026-09-08	✓
187	Критическая	CVE-2026-64047	Linux	Сетевой	ACE	2026-09-08	✓
188	Высокая	BDU:2026-14309	MariaDB	Сетевой	PE	2026-09-09	✓
189	Высокая	CVE-2026-81963	Windows Update Stack	Локальный	PE	2026-09-09	✓
190	Высокая	CVE-2026-85880	Windows Advanced Local Procedure Call	Локальный	PE	2026-09-09	✓
191	Критическая	CVE-2026-64000	Linux	Сетевой	ACE	2026-09-08	✓
192	Критическая	CVE-2026-64132	Linux	Сетевой	ACE	2026-09-08	✓

193	Критическая	CVE-2026-64091	Linux	Сетевой	ACE	2026-09-08	✓
194	Критическая	CVE-2026-63795	Linux	Сетевой	ACE	2026-09-08	✓
195	Высокая	CVE-2026-84309	PyPDF	Сетевой	DoS	2026-09-09	✓
196	Высокая	CVE-2026-63885	Linux	Локальный	ACE	2026-09-08	✓
197	Критическая	CVE-2026-28309	SolarWinds Serv-U	Сетевой	PE	2026-07-23	✓
198	Критическая	CVE-2026-64090	Linux	Сетевой	ACE	2026-09-08	✓
199	Высокая	CVE-2026-63870	Linux	Локальный	ACE	2026-09-08	✓
200	Критическая	CVE-2026-28307	SolarWinds Serv-U	Сетевой	PE	2026-07-23	✓
201	Критическая	CVE-2026-28306	SolarWinds Serv-U	Сетевой	PE	2026-07-23	✓
202	Высокая	CVE-2026-63864	Linux	Локальный	ACE	2026-09-08	✓
203	Высокая	CVE-2026-64045	Linux	Локальный	ACE	2026-09-08	✓
204	Высокая	CVE-2026-63926	Linux	Локальный	ACE	2026-09-08	✓
205	Критическая	CVE-2026-28305	SolarWinds Serv-U	Сетевой	ACE	2026-07-23	✓
206	Высокая	CVE-2026-64135	Linux	Локальный	ACE	2026-09-08	✓
207	Высокая	CVE-2026-64169	Linux	Локальный	ACE	2026-09-08	✓

208	Высокая	CVE-2026-63913	Linux	Сетевой	DoS	2026-09-08	✓
209	Высокая	CVE-2026-63893	Linux	Смежная сеть	DoS	2026-09-08	✓
210	Высокая	CVE-2026-8201	MongoDB Server	Сетевой	ACE	2026-07-15	✓
211	Высокая	CVE-2026-63971	Linux	Локальный	ACE	2026-09-08	✓
212	Высокая	CVE-2026-53401	Linux	Локальный	ACE	2026-09-08	✓
213	Высокая	CVE-2026-63918	Linux	Локальный	ACE	2026-09-08	✓
214	Высокая	CVE-2026-64002	Linux	Локальный	ACE	2026-09-08	✓
215	Высокая	CVE-2026-64008	Linux	Локальный	ACE	2026-09-08	✓
216	Высокая	CVE-2026-64053	Linux	Локальный	ACE	2026-09-08	✓
217	Высокая	CVE-2026-64084	Linux	Локальный	ACE	2026-09-08	✓
218	Высокая	CVE-2026-53386	Linux	Локальный	ACE	2026-09-08	✓
219	Высокая	CVE-2026-63799	Linux	Локальный	ACE	2026-09-08	✓
220	Высокая	CVE-2026-63809	Linux	Локальный	ACE	2026-09-08	✓
221	Высокая	CVE-2026-63824	Linux	Локальный	ACE	2026-09-08	✓
222	Высокая	CVE-2026-63854	Linux	Локальный	ACE	2026-09-08	✓

223	Высокая	CVE-2026-63925	Linux	Смежная сеть	DoS	2026-09-08	✓
224	Не определено	CVE-2026-67281	MikroTik RouterOS	Не определено	ACE	2026-09-07	✓
225	Высокая	CVE-2026-67277	MikroTik RouterOS	Сетевой	DoS	2026-09-07	✓
226	Критическая	CVE-2026-86060	MikroTik RouterOS	Сетевой	PE	2026-09-07	✓
227	Высокая	CVE-2026-67276	MikroTik RouterOS	Сетевой	WLF	2026-09-07	✓
228	Высокая	CVE-2026-20277	Cisco IOS XR Software	Сетевой	ACE	2026-09-02	✓
229	Критическая	CVE-2026-20212	Cisco NX-OS Software	Сетевой	ACE	2026-09-02	✓
230	Высокая	CVE-2026-70468	FortiManager	Сетевой	ACE	2026-08-12	✓

1

Краткое описание: Обход безопасности в XMLDOM

Идентификатор уязвимости: CVE-2026-83609
BDU:2026-14134

Идентификатор программной ошибки: CWE-625 Некорректное ограничение регулярных выражений

Уязвимый продукт: XMLDOM: от 0.9.0 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-3px3-54cx-rmw9
- 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/2026-14134

2

Краткое описание: Отказ в обслуживании в XMLDOM

Идентификатор уязвимости: CVE-2026-83606
BDU:2026-14132

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: OpenShift Container Platform: 4
XMLDOM: от 0.9.0-beta.9 до 0.9.11

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-g53g-w8rj-fmg7
- https://github.com/xmldom/xmldom/commit/73df6b8bdbd86f904b9e8c3ab9c49aa54ef2802e
- https://github.com/xmldom/xmldom/pull/1039
- https://github.com/xmldom/xmldom/releases/tag/0.9.11
- https://access.redhat.com/security/cve/cve-2026-83606
- https://bdu.fstec.ru/vul/2026-14132

Краткое описание: Отказ в обслуживании в gRPC-Go

Идентификатор уязвимости: CVE-2026-84304
BDU:2026-14130

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

Уязвимый продукт: gRPC-Go: до 1.83.1

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

3

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/grpc/grpc-go/security/advisories/GHSA-vp52-pcj8-j9qc
- https://github.com/grpc/grpc-go/commit/7354d9c8debb4bcf2225bf429857078de310c176
- https://github.com/grpc/grpc-go/commit/8cfeca0e1ee5ea0980dcc320e20240fa1079ec77
- https://github.com/grpc/grpc-go/pull/9331
- https://github.com/grpc/grpc-go/pull/9333
- https://github.com/grpc/grpc-go/releases/tag/v1.83.1
- https://dailycve.com/grpc-go-heap-memory-exhaustion-oom-via-http-2-data-frame-fragmentation-cve-2026-84304-high-dc-sep2026-2077/
- https://advisories.gitlab.com/golang/google.golang.org/grpc/CVE-2026-84304/
- https://bdu.fstec.ru/vul/2026-14130

4

Краткое описание: Отказ в обслуживании в Predis

Идентификатор уязвимости: CVE-2026-84372
BDU:2026-14128

Идентификатор программной ошибки: CWE-93 Некорректная нейтрализация последовательностей символов CRLF (внедрение символов CRLF)

Уязвимый продукт: Predis: от 3.0.0-RC1 до 3.3.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

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: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://github.com/predis/predis/security/advisories/GHSA-w6f5-v2h6-g786
- https://github.com/predis/predis/commit/053cb4b6ac7fb1f469ead96a78d059bc0458e408
- https://github.com/predis/predis/issues/1574
- https://github.com/predis/predis/pull/1586
- https://github.com/predis/predis/releases/tag/v3.3.0
- https://bdu.fstec.ru/vul/2026-14128

5

Краткое описание: Отказ в обслуживании в Grafana

Идентификатор уязвимости: CVE-2026-8609
BDU:2026-14126

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

Уязвимый продукт: РЕД ОС: 8.0
Grafana: до 13.0.2

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: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://grafana.com/security/security-advisories/cve-2026-8609/
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8609
- https://bdu.fstec.ru/vul/2026-14126

6

Краткое описание: Повышение привилегий в pgAdmin 4

Идентификатор уязвимости: CVE-2026-7813
BDU:2026-14124

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: РЕД ОС: 8.0
pgAdmin 4: до 9.15

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: 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: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://github.com/pgadmin-org/pgadmin4/pull/9830
- https://github.com/pgadmin-org/pgadmin4/pull/9835
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-7813
- https://bdu.fstec.ru/vul/2026-14124

7

Краткое описание: Выполнение произвольного кода в MongoDB Server

Идентификатор уязвимости: CVE-2026-6914
BDU:2026-14123

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

Уязвимый продукт: РЕД ОС: 8.0
MongoDB Server: до 7.0.32

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: 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://jira.mongodb.org/browse/SERVER-119981
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-6914
- https://bdu.fstec.ru/vul/2026-14123

8

Краткое описание: Отказ в обслуживании в .NET

Идентификатор уязвимости: CVE-2026-57108
BDU:2026-14122

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

Уязвимый продукт: РЕД ОС: 8.0
.NET: от 10.0 до 10.0.10

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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57108
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-57108
- https://bdu.fstec.ru/vul/2026-14122

9

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53268
BDU:2026-14071

Идентификатор программной ошибки: CWE-788 Доступ к областям памяти за пределами буфера

Уязвимый продукт: Linux: от 2.6.20 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53268
- https://git.kernel.org/stable/c/4cdda7f868f48e2f81579371584fdbdce37df2c8
- https://git.kernel.org/stable/c/8a1d6e40dedfe1068aee094d851bd69e289c9fd6
- https://git.kernel.org/stable/c/0afc802160af0df61ed374fdb97fb34cfe5cdf2f
- https://git.kernel.org/stable/c/7c34f91305292083253df6a9f6c8ede02d4ccaea
- https://git.kernel.org/stable/c/ddddd8271359961e403d11c90c9ba9fc38914f7e
- https://git.kernel.org/stable/c/9e5da2379f968a3ea5a6e38921ab6201576466dc
- https://git.kernel.org/stable/c/573810f61bcd6b6815e2ff53bbdd2b9c9d747176

- https://git.kernel.org/linus/66eba0ffce3b7e11449946b4cbbef8ea36112f56
- https://security-tracker.debian.org/tracker/CVE-2026-53268
- https://access.redhat.com/security/cve/CVE-2026-53268
- https://ubuntu.com/security/CVE-2026-53268
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53268
- https://bdu.fstec.ru/vul/2026-14071

10

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53277
BDU:2026-14073

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 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: 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: 8.8 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-2026-53277
- https://git.kernel.org/stable/c/97706097f9b851cfe55c3b00b083dfc2bcf542bc
- https://git.kernel.org/stable/c/ec42b4ed1b072ea2d03f086061aa67bad6d8de39
- https://git.kernel.org/linus/f2ca45b50d4216c9cc7ffabf50d9ad1932209251
- https://security-tracker.debian.org/tracker/CVE-2026-53277
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53277
- https://access.redhat.com/security/cve/CVE-2026-53277
- https://ubuntu.com/security/CVE-2026-53277

- https://bdu.fstec.ru/vul/2026-14073

11

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53281
BDU:2026-14076

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.13.3 до 6.18.32 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-2026-53281
- https://git.kernel.org/stable/c/9022cb9ac0c2a72a57fa8ebf92ac74f953ca0153
- https://git.kernel.org/stable/c/cdfe3c9f2c9e28a8651ee463c88ad191ced2f840
- https://git.kernel.org/linus/79ea2feb917b05366b49d85573c9c5331f043b2c
- https://security-tracker.debian.org/tracker/CVE-2026-53281
- https://access.redhat.com/security/cve/CVE-2026-53281
- https://ubuntu.com/security/CVE-2026-53281
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53281

- https://bdu.fstec.ru/vul/2026-14076

12

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53282
BDU:2026-14077

Идентификатор программной ошибки: CWE-788 Доступ к областям памяти за пределами буфера

Уязвимый продукт: Linux: от 6.14 до 6.18.32 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: 8.0 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-2026-53282
- https://git.kernel.org/stable/c/b0bd7a850e1f082560959707dbf57b0402071646
- https://git.kernel.org/stable/c/7dba9631faa2ee0785e8c2bf0e3d90a05f26dd8c
- https://git.kernel.org/linus/786a45757dcdf8f2beb9d4a6db605db16c18b2b4
- https://ubuntu.com/security/CVE-2026-53282
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53282
- https://bdu.fstec.ru/vul/2026-14077

13

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53290
BDU:2026-14080

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.15 до 6.18.32 включительно
Red Hat Enterprise Linux: 10
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: 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://www.cve.org/CVERecord?id=CVE-2026-53290
- https://git.kernel.org/stable/c/bebce43f34b5feb8a760aa832eba81e0f8a38871
- https://git.kernel.org/stable/c/84f2bfbe6e38f8b9815ca00826e53b7f51420402
- https://git.kernel.org/linus/dc2d9842c67d883d3200ae33b9c3859dd9492408
- https://access.redhat.com/security/cve/CVE-2026-53290
- https://ubuntu.com/security/CVE-2026-53290
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53290
- https://bdu.fstec.ru/vul/2026-14080

14

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53296
BDU:2026-14084

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.4 до 5.10.257 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: 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: 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://www.cve.org/CVERecord?id=CVE-2026-53296
- https://git.kernel.org/stable/c/0ad8c4a03a358de7811ba1ab8cbd1fe76ad0ff6b
- https://git.kernel.org/stable/c/15c4cc3850cfe1b973eb7b63c02314b267f06a64
- https://git.kernel.org/stable/c/187069ccc3474516af32350e20d7e449160fa6de
- https://git.kernel.org/stable/c/81c9e7e4030e71391ab479c4c6e17b64802577aa
- https://git.kernel.org/stable/c/6c6ce2ccb4fcf1617fec83f91b21aa0265f30701
- https://git.kernel.org/stable/c/742001919653e7313b4e91780c5d108be1692365
- https://git.kernel.org/stable/c/02beb178e2e159daeb8f992d7abb16a37da31664

- https://git.kernel.org/linus/c02053a9055d5fdfd32432287cca8958db1d5bc5
- https://security-tracker.debian.org/tracker/CVE-2026-53296
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53296
- https://access.redhat.com/security/cve/CVE-2026-53296
- https://ubuntu.com/security/CVE-2026-53296
- https://bdu.fstec.ru/vul/2026-14084

15

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53262
BDU:2026-14068

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

Уязвимый продукт: Linux: от 2.6.35 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: 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://www.cve.org/CVERecord?id=CVE-2026-53262
- https://git.kernel.org/stable/c/78cdfdca88cbf731a92f3b9ee5427c633dd94e28
- https://git.kernel.org/stable/c/e251d4cdfc725c9e7d686161e3b775a0e7d95053
- https://git.kernel.org/stable/c/62f327e287cf7b595ae3f73ba72f5cd2a9e9f39f
- https://git.kernel.org/linus/a213a8950414c684999dcf03edeea6c46ede172e
- https://security-tracker.debian.org/tracker/CVE-2026-53262
- https://access.redhat.com/security/cve/CVE-2026-53262
- https://ubuntu.com/security/CVE-2026-53262

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53262
- https://bdu.fstec.ru/vul/2026-14068

16

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53145
BDU:2026-14006

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 7.0.9 до 7.0.12 включительно
Red Hat Enterprise Linux: 10
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: 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://www.cve.org/CVERecord?id=CVE-2026-53145
- https://git.kernel.org/stable/c/c0639ede2f24ac224b2079cd35ecd5fd8ad4e3cd
- https://git.kernel.org/stable/c/1d9b93df7fc768228906e24220591ec1cddad391
- https://git.kernel.org/linus/1a4f03d22fb655e5f192244fb2c87d8066fcfca2
- https://access.redhat.com/security/cve/CVE-2026-53145
- https://ubuntu.com/security/CVE-2026-53145
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53145
- https://bdu.fstec.ru/vul/2026-14006

17

Краткое описание: Отказ в обслуживании в Grafana

Идентификатор уязвимости: CVE-2026-33382
BDU:2026-14093

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

Уязвимый продукт: РЕД ОС: 8.0
Grafana: до 13.0.2

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: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://grafana.com/security/security-advisories/cve-2026-33382/
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-33382
- https://bdu.fstec.ru/vul/2026-14093

Краткое описание: Получение конфиденциальной информации в exim

Идентификатор уязвимости: CVE-2026-40684
BDU:2026-14096

Идентификатор программной ошибки: CWE-684 Некорректное обеспечение заявленных функций

Уязвимый продукт: exim: до 4.99.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

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.

18

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://github.com/advisories/GHSA-q496-q274-jgh9
- http://www.openwall.com/lists/oss-security/2026/05/01/11
- https://code.exim.org/exim/exim/commit/628bbaca7672748d941a12e7cd5f0122a4e18c81
- https://exim.org/static/doc/security/CVE-2025-40684.txt
- https://exim.org/static/doc/security/CVE-2026-40684.txt
- https://exim.org/static/doc/security/cve-2026-04.1/CVE2026-40684.assessment
- https://www.openwall.com/lists/oss-security/2026/04/30/21
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-40684
- https://security-tracker.debian.org/tracker/CVE-2026-40684

- https://bdu.fstec.ru/vul/2026-14096

19

Краткое описание: Получение конфиденциальной информации в exim

Идентификатор уязвимости: CVE-2026-40685
BDU:2026-14097

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: exim: до 4.99.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

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: 9.8 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/advisories/GHSA-pph6-fvmv-fjrc
- https://code.exim.org/exim/exim/commit/9fdc057e71b87c87a0d3d2288b2810a0efaaba57
- https://exim.org/static/doc/security/CVE-2025-40685.txt
- https://exim.org/static/doc/security/CVE-2026-40685.txt
- https://exim.org/static/doc/security/cve-2026-04.1/CVE2026-40685.assessment
- https://www.openwall.com/lists/oss-security/2026/04/30/21
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-40685
- https://security-tracker.debian.org/tracker/CVE-2026-40685
- https://bdu.fstec.ru/vul/2026-14097

Краткое описание: Выполнение произвольного кода в ImageMagick

Идентификатор уязвимости: CVE-2026-56372
BDU:2026-14117

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

Уязвимый продукт: ImageMagick: до 7.1.2-19
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

20 **Рекомендации по устранению:** Данная уязвимость устраняется официальным 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-8vfj-q2cp-5m5j
- https://redos.red-soft.ru/search/?iblock_id=24&q=2026-56372
- https://bdu.fstec.ru/vul/2026-14117

21

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53137
BDU:2026-14002

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.6 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: 8.0 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-2026-53137
- https://git.kernel.org/stable/c/3c4444aec06c74fbc05661f370954ac814963c38
- https://git.kernel.org/stable/c/91fb41218c413989d8b6c837748751454b452d68
- https://git.kernel.org/stable/c/964e50ef7b8f09815a7d05b8326af700f8d5bc96
- https://git.kernel.org/stable/c/79e0273272a05fb26f9b1e55bf1a52eefc3b7b35
- https://git.kernel.org/stable/c/bfba882cfcd08f6540f72f48e786b6404f5d2c5b
- https://git.kernel.org/stable/c/1906064d50d194a145486e5caf3db3e708b6f6ef
- https://git.kernel.org/stable/c/98cfb7530ea91d8e5e928285cdce58e1131f6e83

- https://git.kernel.org/linus/f0f3981c43b32cadfe373d636d9e9ca522bb3702
- https://security-tracker.debian.org/tracker/CVE-2026-53137
- https://access.redhat.com/security/cve/CVE-2026-53137
- https://ubuntu.com/security/CVE-2026-53137
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53137
- https://bdu.fstec.ru/vul/2026-14002

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53148
BDU:2026-14008

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.16 до 6.1.175 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.

22

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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53148
- https://git.kernel.org/stable/c/0b334279a82d79fb4723bd4f614305de1ab69caa
- https://git.kernel.org/stable/c/6021d39ccd979713b39b980286020d8f9a45efd1
- https://git.kernel.org/stable/c/89ae04365e01d5ae4aae83044a8bbd2a9aaf8d0d
- https://git.kernel.org/stable/c/5db10c8ad8c09f72c847dfeef3d876098257f505
- https://git.kernel.org/stable/c/05a43157676c243c248d1c6d9dcecbe6eba2f35d
- https://git.kernel.org/stable/c/fcbd0cdab92838854a5818be7ed8a097164ef6d5
- https://git.kernel.org/stable/c/906035d5c3784570191d259cbf9a0ac1617852b5
- https://git.kernel.org/linus/322e93448d908434ae5545660fcbe8f5a7a8e141

- https://security-tracker.debian.org/tracker/CVE-2026-53148
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53148
- https://ubuntu.com/security/CVE-2026-53148
- https://bdu.fstec.ru/vul/2026-14008

23

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53109
BDU:2026-13997

Идентификатор программной ошибки: CWE-590 Освобождение не выделенной динамической памяти

Уязвимый продукт: Linux: от 6.6 до 6.18.32 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 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53109
- https://git.kernel.org/stable/c/c8b710655012a2993a9567873fb71a8a51f8459c
- https://git.kernel.org/stable/c/a32db6fca3c74b4eb8bae5470f0680deb4cbac6f
- https://git.kernel.org/linus/fda4d71651f71c44b35829d13f3c8bf920032f77
- https://security-tracker.debian.org/tracker/CVE-2026-53109
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53109
- https://access.redhat.com/security/cve/CVE-2026-53109
- https://ubuntu.com/security/CVE-2026-53109

- https://bdu.fstec.ru/vul/2026-13997

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52922
BDU:2026-13900

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.19 до 7.0.10 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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.

24

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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52922
- https://git.kernel.org/stable/c/9bcebaedfb8479cb4affb23c7a0d000ca9a20e73
- https://git.kernel.org/stable/c/2edb8aeb3cdda9d00ec4997252dc5bcd6f54d8ef
- https://git.kernel.org/stable/c/ce0c381199402a2c58f4599f4f6ed100d872d0da
- https://git.kernel.org/stable/c/866ac1d57040ed0b44ca732e3c66b3aa6b93011c
- https://git.kernel.org/stable/c/4d420d9ee70a220a2cd95aa0dd2e15acad66a505
- https://git.kernel.org/stable/c/9cceea8eeba710def2a5707ee00f00c74a9a1cac
- https://git.kernel.org/stable/c/cf48e75fc4fe0d5cc7721c82d454221d01367b93
- https://git.kernel.org/linus/2d8826a2d3657cea66fb0370f9e521575a673871

- https://security-tracker.debian.org/tracker/CVE-2026-52922
- https://ubuntu.com/security/CVE-2026-52922
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52922
- https://bdu.fstec.ru/vul/2026-13900

25

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52924
BDU:2026-13901

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.16 до 6.1.175 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-2026-52924
- https://git.kernel.org/stable/c/84b7a319105db2f917ccdcf502bdc866082b1285
- https://git.kernel.org/stable/c/f46e1d1a758878f0d22c4fbbd1bf42bb7165d1e8
- https://git.kernel.org/stable/c/3c0741a441a7df7099d7ca6a64a6a0de09c677c8
- https://git.kernel.org/stable/c/2afc9e684dc7fecf73db1edc937ebbc47b4b68dc
- https://git.kernel.org/stable/c/1d4652f677906a64487c13f9ace54b0eb263b5d0
- https://git.kernel.org/stable/c/a6207349e703cfc04756a4d16dec9176135813a5
- https://git.kernel.org/stable/c/83ade59e5da365f4bf8bce72c5a38774202b442f

- https://git.kernel.org/linus/e374b22e9b07b72a25909621464ff74096151bfb
- https://security-tracker.debian.org/tracker/CVE-2026-52924
- https://access.redhat.com/security/cve/CVE-2026-52924
- https://ubuntu.com/security/CVE-2026-52924
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52924
- https://github.com/Eliot-code/CVE-2026-52924
- https://bdu.fstec.ru/vul/2026-13901

26

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52927
BDU:2026-13903

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 6.13 до 6.18.34 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: 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://www.cve.org/CVERecord?id=CVE-2026-52927
- https://git.kernel.org/stable/c/d7a8fb6f10d55a1c37b0bf8c20cca24dffd76e00
- https://git.kernel.org/stable/c/21af4c030567d2e6c89bb927bc18b51fba52a400
- https://git.kernel.org/stable/c/dad9ebf8107955bb54bd3f9cf22591b6ff37bac1
- https://git.kernel.org/stable/c/a27cb7325a6c69970041c7f8541fafed5a1ea3ec
- https://git.kernel.org/stable/c/7ad0e463fc7eafae2141cc38054264636f8b3e94
- https://git.kernel.org/stable/c/bf8e8eac7ede51dc318e06acef5a896dcbba7595
- https://git.kernel.org/stable/c/fcc4c043d137e7f1de4673dba1f3116e45377c67

- https://git.kernel.org/linus/f438d1786d657d57790c5d138d6db3fc9fdac392
- https://security-tracker.debian.org/tracker/CVE-2026-52927
- https://access.redhat.com/security/cve/CVE-2026-52927
- https://ubuntu.com/security/CVE-2026-52927
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52927
- https://bdu.fstec.ru/vul/2026-13903

27

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52929
BDU:2026-13905

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.16 до 6.1.175 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52929
- https://git.kernel.org/stable/c/0cd2dc6dce8ca47212cd306ccd52eb315ef3cf85
- https://git.kernel.org/stable/c/a6724b7b812ac8793514a1d5938db5d9d29ae725
- https://git.kernel.org/stable/c/9662eb0401518f0b4681f10e7fbf688f504f24cf
- https://git.kernel.org/stable/c/7dd9a42b044aad2dbe037db1c1e2943582485b44
- https://git.kernel.org/stable/c/39dc2b0eb5371a669ebc9ec6072b9184eac95418
- https://git.kernel.org/stable/c/d5ea0b3e261fcb2cfff142675516165244cab1da
- https://git.kernel.org/stable/c/1c6773b8c081509dcd5cd2954f2b02c50c00f151

- https://git.kernel.org/linus/a5f8a90ac9f77c678a9781c0a464b635e0d63e49
- https://security-tracker.debian.org/tracker/CVE-2026-52929
- https://access.redhat.com/security/cve/CVE-2026-52929
- https://ubuntu.com/security/CVE-2026-52929
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52929
- https://bdu.fstec.ru/vul/2026-13905

28

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52932
BDU:2026-13907

Идентификатор программной ошибки: CWE-772 Удержание ресурса после его использования

Уязвимый продукт: Linux: от 6.19 до 7.0.11 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52932
- https://git.kernel.org/stable/c/dc6dcba80d72a27ab61831ad3d253316e0c9b9d5
- https://git.kernel.org/stable/c/b30aa173c3809f6af4c83a86099be1be19aa48eb
- https://git.kernel.org/linus/7dbac7680eb629b3b4dc7e98c34f943b8814c0c8
- https://ubuntu.com/security/CVE-2026-52932
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52932
- https://bdu.fstec.ru/vul/2026-13907

29

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52935
BDU:2026-13908

Идентификатор программной ошибки: CWE-788 Доступ к областям памяти за пределами буфера

Уязвимый продукт: Linux: от 5.6 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: 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://www.cve.org/CVERecord?id=CVE-2026-52935
- https://git.kernel.org/stable/c/6564e9c7af7e1dc7bfe7f3093b728abe484d7630
- https://git.kernel.org/stable/c/1777ceac4bea5e568a5ad44b7f9bb219c1db21b6
- https://git.kernel.org/stable/c/8c6c691bf062dc0753a139a4ab8cb92a70fcf8f3
- https://git.kernel.org/stable/c/aa82a078f70f7ff88ba7d1017134e79d1ac140f2
- https://git.kernel.org/stable/c/ba21439302db9a82fe4edbed1e38a97271529421
- https://git.kernel.org/stable/c/f9b38a8fbfa07f1deaf7ee1eb38fa8b21ea13990
- https://git.kernel.org/stable/c/37487d55bf3300e3d2c1368da5c2bd3e3834ea4f

- https://git.kernel.org/linus/c381039ade2e161ab08c0eda73c4f8b9a7115928
- https://security-tracker.debian.org/tracker/CVE-2026-52935
- https://access.redhat.com/security/cve/CVE-2026-52935
- https://ubuntu.com/security/CVE-2026-52935
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52935
- https://bdu.fstec.ru/vul/2026-13908

30

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53135
BDU:2026-14001

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.2 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: 8.0 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-2026-53135
- https://git.kernel.org/stable/c/ee9cfcf77a8e8af637396dc00966df5f701e661c
- https://git.kernel.org/stable/c/b781f90a9528555c709e59789550893581ef0be4
- https://git.kernel.org/stable/c/a2de1d71891a038a9346b2c1a72b88c8350f2479
- https://git.kernel.org/stable/c/7fc4fab4acc307ad2903312c195872b2953d32c3
- https://git.kernel.org/stable/c/7ae95c0275c330b5dbae806f8e431720edad776f
- https://git.kernel.org/stable/c/bb6f705b73b5f191f14ad004e2c8c4b615806187
- https://git.kernel.org/stable/c/c90954cdea4d6998ec345de0d840d030c145b89e

- https://git.kernel.org/linus/adf67034b1f61f7119295208085bfd43f85f56af
- https://security-tracker.debian.org/tracker/CVE-2026-53135
- https://access.redhat.com/security/cve/CVE-2026-53135
- https://ubuntu.com/security/CVE-2026-53135
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53135
- https://bdu.fstec.ru/vul/2026-14001

31

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52951
BDU:2026-13918

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.8 до 6.12.90 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 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: 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:

- чhttps://www.cve.org/CVERecord?id=CVE-2026-52951
- https://git.kernel.org/stable/c/9894731e513019df22a29e5c52f1c98890355ff1
- https://git.kernel.org/stable/c/20a99ea1e2fd720856d6ba497ff26b82c604751f
- https://git.kernel.org/stable/c/c473ae25421fddc3dde247ba7b85225b10641d09
- https://git.kernel.org/linus/981bedbbe61364fcc3a3b87ebaf648a66cd07108
- https://security-tracker.debian.org/tracker/CVE-2026-52951
- https://access.redhat.com/security/cve/CVE-2026-52951
- https://ubuntu.com/security/CVE-2026-52951

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52951
- https://bdu.fstec.ru/vul/2026-13918

32

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52952
BDU:2026-13919

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 7.0 до 7.0.9 включительно
Red Hat Enterprise Linux: 10
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-2026-52952
- https://git.kernel.org/stable/c/8fc289e809f3eb7e36cadc4684ab6fad747a5a93
- https://git.kernel.org/linus/5474e6e17a262db45c60575c73f70210f5c7001f
- https://access.redhat.com/security/cve/CVE-2026-52952
- https://ubuntu.com/security/CVE-2026-52952
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52952
- https://bdu.fstec.ru/vul/2026-13919

33

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52954
BDU:2026-13920

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Linux: от 4.13 до 5.10.257 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52954
- https://git.kernel.org/stable/c/c7bf7864e2924fa5508ac270b0e9364bc13d5a6c
- https://git.kernel.org/stable/c/f47430fc1f815e87406e2d3b4e476eff1bc7fd9b
- https://git.kernel.org/stable/c/0b6a3bcb91bc5bfeda39f0df3b71bab62c13e9da
- https://git.kernel.org/stable/c/534ebc08df97c47d4c7596f336fa31ecbf91519c
- https://git.kernel.org/stable/c/80c73bd1b2b04355d1d0c29be8ccbd25a380905d
- https://git.kernel.org/stable/c/4d2b37abda9536808655830d683dc491d31741a8
- https://git.kernel.org/stable/c/0a1265a9ab875f92b6a3ffb497404f46cf9d76a3

- https://git.kernel.org/linus/d289478cfc0bcf81c7914200d6abdcb78bd04ded
- https://security-tracker.debian.org/tracker/CVE-2026-52954
- https://access.redhat.com/security/cve/CVE-2026-52954
- https://ubuntu.com/security/CVE-2026-52954
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52954
- https://bdu.fstec.ru/vul/2026-13920

34

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52955
BDU:2026-13921

Идентификатор программной ошибки: CWE-188 Некорректные предположения о схеме организации данных или памяти

Уязвимый продукт: Linux: от 2.6.34 до 5.10.257 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-2026-52955
- https://git.kernel.org/stable/c/6e70ef53e818c53eab28d7b0026b7fd03dddaba5
- https://git.kernel.org/stable/c/ebe76d58a48a48031b98543d86c4cd30a825b622
- https://git.kernel.org/stable/c/3f42508191e129ee6b5ea96578d5cab14f2a013a
- https://git.kernel.org/stable/c/ea0d42137f0c06da71e37ffc647aab4c5309599a
- https://git.kernel.org/stable/c/cceb10023e76bc89f3fe9238ebd0ccab0fc7c7c5
- https://git.kernel.org/stable/c/0f3604cbe4df14c5e58288ac9f57511e726a222d
- https://git.kernel.org/stable/c/fb176a99e4c1a5a8448a83d83d3606203ba81faa

- https://git.kernel.org/linus/4c79fc2d598694bda845b46229c9d48b65042970
- https://security-tracker.debian.org/tracker/CVE-2026-52955
- https://access.redhat.com/security/cve/CVE-2026-52955
- https://ubuntu.com/security/CVE-2026-52955
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52955
- https://bdu.fstec.ru/vul/2026-13921

35

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52956
BDU:2026-13922

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 4.9.6 до 7.0.9 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52956
- https://git.kernel.org/stable/c/c7e9b53aebe401970f1b5f5a01b4e021b18e8bb2
- https://git.kernel.org/linus/821365487aa58d06bda65c676ba215d506ba9768
- https://security-tracker.debian.org/tracker/CVE-2026-52956
- https://access.redhat.com/security/cve/CVE-2026-52956
- https://ubuntu.com/security/CVE-2026-52956
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52956
- https://bdu.fstec.ru/vul/2026-13922

36

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52957
BDU:2026-13923

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 4.13 до 5.10.257 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52957
- https://git.kernel.org/stable/c/d55ffad8d422b5d1cc44dad32bd3d25f4471cd9f
- https://git.kernel.org/stable/c/301286c0ccd37d66b0e40786fd35a4f19cdbd88a
- https://git.kernel.org/stable/c/7169f326a23d0f547fcd90e68b72fd387622e126
- https://git.kernel.org/stable/c/d7a65a34d2453f8cd3e0cc0e1319740af7e24276
- https://git.kernel.org/stable/c/312ec973efac0efb9b9ed64214235910e9ecbaa8
- https://git.kernel.org/stable/c/f2f95e6d4b97e70bb876139b0583fc8079983f85
- https://git.kernel.org/stable/c/a20e16ebfe2fa65348eb4b2dc7deac330ce03e9c

- https://git.kernel.org/linus/28b0a2ab8c82d0bbdeb8013029c67c978ce6e4bf
- https://security-tracker.debian.org/tracker/CVE-2026-52957
- https://access.redhat.com/security/cve/CVE-2026-52957
- https://ubuntu.com/security/CVE-2026-52957
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52957
- https://bdu.fstec.ru/vul/2026-13923

37

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52950
BDU:2026-13917

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.18 до 6.18.32 включительно
Red Hat Enterprise Linux: 10
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: 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://www.cve.org/CVERecord?id=CVE-2026-52950
- https://git.kernel.org/stable/c/39fdac6be02eb7c3460518c1c4085f75f935c4ce
- https://git.kernel.org/stable/c/827062952ed9bdf4220466c1f05ce452d04bdedf
- https://git.kernel.org/linus/155a372a1cc50fa93387c5d3cdfd614a61e1afd1
- https://access.redhat.com/security/cve/CVE-2026-52950
- https://ubuntu.com/security/CVE-2026-52950
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52950
- https://bdu.fstec.ru/vul/2026-13917

38

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52958
BDU:2026-13924

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 5.3 до 5.10.257 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-2026-52958
- https://git.kernel.org/stable/c/36a79759a288961b1ff28a68ec2d1f56f6848098
- https://git.kernel.org/stable/c/3f2575bb7f955d42569d96c3e04fa958a0dcf4b4
- https://git.kernel.org/stable/c/8713bbc4b2b9ad78f803978e54b7e49dd21bd9be
- https://git.kernel.org/stable/c/0d2dd7e6bb74fd7712aa73457a4a821906c6863a
- https://git.kernel.org/stable/c/e7187f33c02488697ec0d01d82bf7a3f8deaba8f
- https://git.kernel.org/stable/c/48df98d12b15360cd56af5c1f460307b340c1197
- https://git.kernel.org/stable/c/ee933694645dac062d65fc2743f92bc06fa0db6b

- https://git.kernel.org/linus/35d0ed82d03e5ee77ea4f31f20e29562a7721649
- https://security-tracker.debian.org/tracker/CVE-2026-52958
- https://access.redhat.com/security/cve/CVE-2026-52958
- https://ubuntu.com/security/CVE-2026-52958
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52958
- https://bdu.fstec.ru/vul/2026-13924

39

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52920
BDU:2026-13898

Идентификатор программной ошибки: CWE-551 Некорректный порядок действий: авторизация до обработки и нормализации

Уязвимый продукт: Linux: от 2.6.17 до 5.10.257 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: 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: 8.3 AV:N/AC:L/PR:L/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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52920
- https://git.kernel.org/stable/c/eb323f7b82d2e2f638de0cc2a177803eb20e0707
- https://git.kernel.org/stable/c/fc1c518bb1f054831ecabb32da9b8e1dff9699c6
- https://git.kernel.org/stable/c/f98b7f85e04b40e28b08c461ded0cc79f14f5509
- https://git.kernel.org/stable/c/82664d0f1ba25e4f9a71994954abae24c60f4067
- https://git.kernel.org/stable/c/b130a6eefa02bd4d475f2f059da8bcfb3e7d18d9
- https://git.kernel.org/stable/c/938867e870fb5471bb16f442aeac81326e05bf65
- https://git.kernel.org/stable/c/392cc1d8408b5665215c1e9290bbf0f92339b043

- https://git.kernel.org/linus/4b2b4d7d4e203c92db8966b163edfacb1f0e1e29
- https://security-tracker.debian.org/tracker/CVE-2026-52920
- https://access.redhat.com/security/cve/CVE-2026-52920
- https://ubuntu.com/security/CVE-2026-52920
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52920
- https://bdu.fstec.ru/vul/2026-13898

40

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46332
BDU:2026-13893

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Linux: от 6.12 до 6.12.85 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: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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46332
- https://git.kernel.org/stable/c/663c2728a6d0f781044431111b53a27f71027e48
- https://git.kernel.org/stable/c/fb91d4e49fcbea0b5091394ac5b8f7d4124265c3
- https://git.kernel.org/stable/c/0339a746ff7cd3f9d10f565e89c99dc93191e58d
- https://git.kernel.org/linus/1214bf28965ceaf584fb20d357731264dd2e10e1
- https://security-tracker.debian.org/tracker/CVE-2026-46332
- https://ubuntu.com/security/CVE-2026-46332
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-46332

- https://bdu.fstec.ru/vul/2026-13893

41

Краткое описание: Внедрение кода в Linux

Идентификатор уязвимости: CVE-2026-63828
BDU:2026-13855

Идентификатор программной ошибки: CWE-1052 Чрезмерное использование жестко закодированных литералов для инициализации

Уязвимый продукт: Linux: от 6.19 до 7.1.2 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Внедрение 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:L/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63828
- https://git.kernel.org/linus/4d587cd8a72155089a627130bbd4716ec0856e21
- https://git.kernel.org/stable/c/7f57428ce00891d26b0f087ef754a4d820ec83aa
- https://git.kernel.org/stable/c/faea60deaa05c76f0772650f42eafde12bd39d93
- https://git.kernel.org/stable/c/07b71c342382b854ab8030b244aeab6a7228ad7d
- https://git.kernel.org/stable/c/4a69b83045d3195d5b9a9b053ad840ddb2998b4e
- https://git.kernel.org/stable/c/45ebb934ea50b436ce49b2f159f090dab0d7fa28
- https://security-tracker.debian.org/tracker/CVE-2026-63828

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63828
- https://ubuntu.com/security/CVE-2026-63828
- https://github.com/4n4s4zi/tfo-connect-bypass
- https://bdu.fstec.ru/vul/2026-13855

42

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53363
BDU:2026-13856

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

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 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://www.cve.org/CVERecord?id=CVE-2026-53363
- https://git.kernel.org/linus/e9096a5a170e7ecd6467bc2e08668ec39897cda7
- https://git.kernel.org/stable/c/dd66f7f6e360ee82cd905517726f8e9091265de5
- https://git.kernel.org/stable/c/c885d111ed9f5a0a1f3cc4e87a50db6518abaa6c
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53363
- https://ubuntu.com/security/CVE-2026-53363
- https://bdu.fstec.ru/vul/2026-13856

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53355
BDU:2026-13857

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.9.54 до 4.10
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.

43

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.cve.org/CVERecord?id=CVE-2026-53355
- https://git.kernel.org/stable/c/66cccec111421a10efdc2c74499d15b93e7acae5
- https://git.kernel.org/stable/c/2c5e5e4a5970c41f16e3ad801a78719ed5d5c71b
- https://git.kernel.org/stable/c/29d940026dce39e3018dab6f67c9427249321270
- https://git.kernel.org/stable/c/e7cf30aa5f1fc6c2a86df65df8b731df20e44d79
- https://git.kernel.org/stable/c/f16ad421a4e3e7db2d14bdf3b16f583bc4f3b30a
- https://git.kernel.org/stable/c/1d4ec754ee3871f7e3670c67bb0298c9c5760926
- https://git.kernel.org/stable/c/27040bbca289a704eafcacca167d310c6ce2b1bc
- https://git.kernel.org/linus/20cf0fb715c41111469577e85e35d15f099473e0

- https://security-tracker.debian.org/tracker/CVE-2026-53355
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53355
- https://ubuntu.com/security/CVE-2026-53355
- https://bdu.fstec.ru/vul/2026-13857

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53343
BDU:2026-13863

Идентификатор программной ошибки: CWE-468 Некорректное масштабирование указателей

Уязвимый продукт: Linux: от 6.12.4 до 6.12.93 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.

44 **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: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53343
- https://git.kernel.org/stable/c/c0b8c148a7754826156993ed6442d31536ec86b4
- https://git.kernel.org/stable/c/c2e3aadc8fef7da068490597fc5582f8f362aeb2
- https://git.kernel.org/stable/c/c74990828d3c486ee44aaa68240eb3abff289d1c
- https://git.kernel.org/stable/c/517720913bd3c17a52cd55a740064f68455ab88e
- https://git.kernel.org/stable/c/2a4dc9a0ac3326e79fb58fdaae724b92127709a9
- https://git.kernel.org/linus/77a1f6883dc6e837bb2cb30b9b02e2f94338e2c6
- https://security-tracker.debian.org/tracker/CVE-2026-53343
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53343

- https://ubuntu.com/security/CVE-2026-53343
- https://bdu.fstec.ru/vul/2026-13863

45

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53329
BDU:2026-13870

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.16 до 6.1.175 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: 8.0 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: 2026-08-31 / 2026-08-31

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53329
- https://git.kernel.org/stable/c/31180638a33acad12c863132704a76536fb66211
- https://git.kernel.org/stable/c/b15825deac1acff72638bbc8f05b89ceef8dfb13
- https://git.kernel.org/stable/c/201151e120f0062bcda21cad5d007b82725ad23b
- https://git.kernel.org/stable/c/a914aa802669e073f014dae2e5708633b5cecd34
- https://git.kernel.org/stable/c/e09689286385a66311ac6922af95339d7a3cef8d
- https://git.kernel.org/stable/c/de988c7a31f0774f07894cfe4802996f318e2870
- https://git.kernel.org/linus/da48bc4461b8a5ebfb9264c9b191a701d8e99009

- https://security-tracker.debian.org/tracker/CVE-2026-53329
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53329
- https://access.redhat.com/security/cve/CVE-2026-53329
- https://ubuntu.com/security/CVE-2026-53329
- https://bdu.fstec.ru/vul/2026-13870

46

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53322
BDU:2026-13873

Идентификатор программной ошибки: CWE-826 Преждевременное освобождение ресурса

Уязвимый продукт: Linux: от 6.19 до 7.0.9 включительно
Red Hat Enterprise Linux: 10
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: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-2026-53322
- https://git.kernel.org/stable/c/4f1000a30f67cf7d328059242776a858611d5ef9
- https://git.kernel.org/linus/d97708701434ce72968e771976aaf9d3438fcafd
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53322
- https://access.redhat.com/security/cve/CVE-2026-53322
- https://ubuntu.com/security/CVE-2026-53322
- https://bdu.fstec.ru/vul/2026-13873

47

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52909
BDU:2026-13895

Идентификатор программной ошибки: CWE-665 Некорректная инициализация

Уязвимый продукт: Linux: от 3.15 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: 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://git.kernel.org/linus/d289d5307762d1838aaece22c6b6fcad9e8865f9
- https://www.cve.org/CVERecord?id=CVE-2026-52909
- https://git.kernel.org/stable/c/ecf8904067dcba0dad86ece80874841e60317885
- https://git.kernel.org/stable/c/dcdce3bc9f08026ff3739ee7339e1bef526fc5f3
- https://security-tracker.debian.org/tracker/CVE-2026-52909
- https://access.redhat.com/security/cve/CVE-2026-52909
- https://ubuntu.com/security/CVE-2026-52909
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52909

- https://bdu.fstec.ru/vul/2026-13895

48

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46288
BDU:2026-13876

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

Уязвимый продукт: Linux: от 6.12 до 6.12.85 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: 8.4 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46288
- https://git.kernel.org/stable/c/37318d1a27c9cc5a70d3cd7e49e30ec86f2b8ca1
- https://git.kernel.org/stable/c/7f0f0926f3010b10cff5e93446258f971e42f2fd
- https://git.kernel.org/stable/c/6fdad20b7975bdc32e85b45f8f7c640f6687b81f
- https://git.kernel.org/linus/faecdd423c27f0d6090156a435ba9dbbac0eaddb
- https://security-tracker.debian.org/tracker/CVE-2026-46288
- https://ubuntu.com/security/CVE-2026-46288
- https://bdu.fstec.ru/vul/2026-13876

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46301
BDU:2026-13879

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 3.1 до 5.10.257 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.

49

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46301
- https://git.kernel.org/stable/c/43334836b907adc21eab3079d2e6b26754468786
- https://git.kernel.org/stable/c/36e58c436d2c2a797800427dc04d74ffd8b6ce1c
- https://git.kernel.org/stable/c/4ca90deeca1c7dd72c1c380ba8143565516def2d
- https://git.kernel.org/stable/c/d79e92161b65832e0b8cad5f3d84d17e5cd7a970
- https://git.kernel.org/stable/c/8822980668c96b5aa251c1e2daec1873262b8f3f
- https://git.kernel.org/stable/c/d50ef3553acbacce6f2843304d41d06dca358bb6
- https://git.kernel.org/stable/c/0e8e57f9737ea257634db1d152fc430a0788a3e1
- https://git.kernel.org/linus/9d72732fe70c11424bc90ed466c7ccfa58b42a9a

- https://security-tracker.debian.org/tracker/CVE-2026-46301
- https://ubuntu.com/security/CVE-2026-46301
- https://bdu.fstec.ru/vul/2026-13879

50

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46304
BDU:2026-13881

Идентификатор программной ошибки: CWE-833 Взаимоблокировка

Уязвимый продукт: Linux: от 4.9.68 до 5.10.257 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: 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://www.cve.org/CVERecord?id=CVE-2026-46304
- https://git.kernel.org/stable/c/ae5b0cad163833e10b271e9becc05d81dae56e5f
- https://git.kernel.org/stable/c/8d66ba89480ff098a58d79003a505f383aa4e920
- https://git.kernel.org/stable/c/a696fbbd5240b4ac9b166f7bd4c550882ff543f1
- https://git.kernel.org/stable/c/9a4d7222c0955b221e38bb66d10e6bccb672c8a1
- https://git.kernel.org/stable/c/ee6e20c4bc9eae542a0954a368449532383169d4
- https://git.kernel.org/stable/c/781f47d641432c26c19625b2cdd7f40825097592
- https://git.kernel.org/stable/c/551f445a56a11a6457550cddcf39c9ebb8bcacc6

- https://git.kernel.org/linus/aade8abd8b868b6ffa9697aadaea28ec7f65bee6
- https://security-tracker.debian.org/tracker/CVE-2026-46304
- https://access.redhat.com/security/cve/CVE-2026-46304
- https://ubuntu.com/security/CVE-2026-46304
- https://bdu.fstec.ru/vul/2026-13881

51

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46308
BDU:2026-13882

Идентификатор программной ошибки: CWE-826 Преждевременное освобождение ресурса

Уязвимый продукт: Linux: от 6.18 до 6.18.29 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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46308
- https://git.kernel.org/stable/c/cb27e43c0511e9e1ca8818d231656070b11c18cf
- https://git.kernel.org/stable/c/38d8410021b55d226847b2ac8d189d89fe5a8866
- https://git.kernel.org/linus/ec1fcddb3117d9452210e838fd37389ee61e10e8
- https://ubuntu.com/security/CVE-2026-46308
- https://bdu.fstec.ru/vul/2026-13882

52

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46311
BDU:2026-13884

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.16 до 7.0.8 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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46311
- https://git.kernel.org/stable/c/336a9186f3a4b65bbd865d93936605ac8a1a3991
- https://git.kernel.org/linus/6da7b1242da4455b11c24ce667d1cab1a348c8ea
- https://security-tracker.debian.org/tracker/CVE-2026-46311
- https://access.redhat.com/security/cve/CVE-2026-46311
- https://ubuntu.com/security/CVE-2026-46311
- https://bdu.fstec.ru/vul/2026-13884

53

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46317
BDU:2026-13888

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.11 до 6.18.34 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46317
- https://git.kernel.org/stable/c/918450ad6010df6ecd2efde12a1409e011da22d6
- https://git.kernel.org/stable/c/4424dbcb06d68e34e51c019a5781a7dc00731971
- https://git.kernel.org/linus/70543358fa08e0f7cebc3447c3b70fe97ad7aaa8
- https://security-tracker.debian.org/tracker/CVE-2026-46317
- https://access.redhat.com/security/cve/CVE-2026-46317
- https://ubuntu.com/security/CVE-2026-46317
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-46317

- https://bdu.fstec.ru/vul/2026-13888

54

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46319
BDU:2026-13889

Идентификатор программной ошибки: CWE-826 Преждевременное освобождение ресурса

Уязвимый продукт: Linux: от 5.7 до 5.10.257 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: 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://www.cve.org/CVERecord?id=CVE-2026-46319
- https://git.kernel.org/stable/c/ece578ca61e572df96cfc80456357ebfae0b4b9e
- https://git.kernel.org/stable/c/a2e0c045c87aa252eb61412e67dd91f2c2b19f81
- https://git.kernel.org/stable/c/67c9ecc9f2575273ed1323e312881fc98ac83d6d
- https://git.kernel.org/stable/c/f23424a0ddadb494d4bd57056a7ca703312d3a7b
- https://git.kernel.org/stable/c/17dfb67cb399b660105d9a8c6100851c0d0cdc70
- https://git.kernel.org/stable/c/4c727c6967a41b37efe0f26332ca9ec5b74785a3
- https://git.kernel.org/stable/c/3e20e1b3058e0b94638e7b931c138e840e266724

- https://git.kernel.org/linus/f462dca0c8415bf0058d0ffa476354c4476d0f09
- https://security-tracker.debian.org/tracker/CVE-2026-46319
- https://access.redhat.com/security/cve/CVE-2026-46319
- https://ubuntu.com/security/CVE-2026-46319
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-46319
- https://bdu.fstec.ru/vul/2026-13889

55

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46290
BDU:2026-13877

Идентификатор программной ошибки: CWE-663 Использование нереентерабельной функции в параллельном контексте

Уязвимый продукт: Linux: от 6.15 до 6.18.29 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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46290
- https://git.kernel.org/stable/c/22b365ba1af3d8c6036b8e5112fffe80998b85a0
- https://git.kernel.org/stable/c/db155b86d1523e85941f61efd7d7ffb594cc9a29
- https://git.kernel.org/linus/088f65e206087bf903743bd18417261d7a4c9644
- https://ubuntu.com/security/CVE-2026-46290
- https://bdu.fstec.ru/vul/2026-13877

56

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52959
BDU:2026-13925

Идентификатор программной ошибки: CWE-239 Некорректная обработка неполных элементов

Уязвимый продукт: Linux: от 6.13.8 до 6.18.32 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: 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://www.cve.org/CVERecord?id=CVE-2026-52959
- https://git.kernel.org/stable/c/3f6fb0211b39aaa1b841260681dd02ca6b693ed5
- https://git.kernel.org/stable/c/9e48b4f813d2c3db75d522aa82ab705ce04b7e2d
- https://git.kernel.org/linus/23e6a1ca04ae44806439a5a446e62e4d42e80bb4
- https://ubuntu.com/security/CVE-2026-52959
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52959
- https://bdu.fstec.ru/vul/2026-13925

57

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52947
BDU:2026-13914

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

Уязвимый продукт: Linux: от 4.7 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 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: 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://www.cve.org/CVERecord?id=CVE-2026-52947
- https://git.kernel.org/stable/c/2aa4c12723fe432e623462a3be42a197a128722b
- https://git.kernel.org/stable/c/03bfa95e452e2b6ccd76a332060ae4feaf5ad84d
- https://git.kernel.org/stable/c/474293d90880622fde9d2430fb0165767090f7b3
- https://git.kernel.org/stable/c/2047c2aa0963bb2872fd722300a15bcb441a4c00
- https://git.kernel.org/stable/c/7de2d447072be3b1a76793f034432338fc9c494b
- https://git.kernel.org/stable/c/ab269990ed58143a92a263be1bee626d82ac03da
- https://git.kernel.org/stable/c/3b20ec8f31e8a6a6782243f473b0abd3463621df

- https://git.kernel.org/linus/a2171131ecda1ed61a594a1eb715e75fdad0fef5
- https://security-tracker.debian.org/tracker/CVE-2026-52947
- https://access.redhat.com/security/cve/CVE-2026-52947
- https://ubuntu.com/security/CVE-2026-52947
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52947
- https://bdu.fstec.ru/vul/2026-13914

58

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52973
BDU:2026-13930

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.17 до 6.18.32 включительно
Red Hat Enterprise Linux: 10
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: 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://www.cve.org/CVERecord?id=CVE-2026-52973
- https://git.kernel.org/stable/c/1dcd36420af2da5bd59306dba9caf78e3d248b1d
- https://git.kernel.org/stable/c/974ac49a9a068b0591a59f65c63eb06579a13091
- https://git.kernel.org/linus/ee9dce44362b2d8132c32964656ab6dff7dfbc6a
- https://access.redhat.com/security/cve/CVE-2026-52973
- https://ubuntu.com/security/CVE-2026-52973
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52973
- https://bdu.fstec.ru/vul/2026-13930

59

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53094
BDU:2026-13993

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.3 до 6.6.140 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: 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://www.cve.org/CVERecord?id=CVE-2026-53094
- https://git.kernel.org/stable/c/a713b72ff88cdab4d5d692908ab1259ada511f4d
- https://git.kernel.org/stable/c/25484c39d1ec82a0368798d956da3de5039b3fe8
- https://git.kernel.org/stable/c/059525cf18e69a9313baf947d8898c6ee7ca6b65
- https://git.kernel.org/stable/c/c79f8503d83d4665be461fb9e45e215d0380c67b
- https://git.kernel.org/linus/a1aa9ef47c299c5bbc30594d3c2f0589edf908e6
- https://security-tracker.debian.org/tracker/CVE-2026-53094
- https://access.redhat.com/security/cve/CVE-2026-53094

- https://ubuntu.com/security/CVE-2026-53094
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53094
- https://bdu.fstec.ru/vul/2026-13993

60

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53092
BDU:2026-13992

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: Linux: от 6.12 до 6.18.32 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 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: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-2026-53092
- https://git.kernel.org/stable/c/d88e8e4a3b52bd5b2ff3eceba4b29d1b5506d066
- https://git.kernel.org/stable/c/cc86a8b0a1c54d2bccf6f68cf49b82dea91b84de
- https://git.kernel.org/linus/d7f14173c0d5866c3cae759dee560ad1bed10d2e
- https://security-tracker.debian.org/tracker/CVE-2026-53092
- https://access.redhat.com/security/cve/CVE-2026-53092
- https://ubuntu.com/security/CVE-2026-53092
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53092

- https://bdu.fstec.ru/vul/2026-13992

61

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53091
BDU:2026-13991

Идентификатор программной ошибки: CWE-188 Некорректные предположения о схеме организации данных или памяти

Уязвимый продукт: Linux: от 3.16 до 7.0.9 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: 8.4 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/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-2026-53091
- https://git.kernel.org/stable/c/9d4f5c68f5ad4ab425f3ce1500c97c9f9743999a
- https://git.kernel.org/linus/7fb4c19670110f052c04e1ec1d2b953b9f4f57e4
- https://security-tracker.debian.org/tracker/CVE-2026-53091
- https://access.redhat.com/security/cve/CVE-2026-53091
- https://ubuntu.com/security/CVE-2026-53091
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53091
- https://bdu.fstec.ru/vul/2026-13991

62

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53090
BDU:2026-13990

Идентификатор программной ошибки: CWE-390 Обнаружение ошибки без реагирования на нее

Уязвимый продукт: Linux: от 5.10 до 7.0.9 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 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: 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://www.cve.org/CVERecord?id=CVE-2026-53090
- https://git.kernel.org/stable/c/d846d83bdacbd8f14fc45c63b8c1d22608452e1c
- https://git.kernel.org/linus/ee861486e377edc55361c08dcbceab3f6b6577bd
- https://security-tracker.debian.org/tracker/CVE-2026-53090
- https://access.redhat.com/security/cve/CVE-2026-53090
- https://ubuntu.com/security/CVE-2026-53090
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53090
- https://bdu.fstec.ru/vul/2026-13990

63

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53085
BDU:2026-13989

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 7.0.9 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: 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://www.cve.org/CVERecord?id=CVE-2026-53085
- https://git.kernel.org/stable/c/239cec25a22662dbd80f57d94b38178c8be95269
- https://git.kernel.org/stable/c/d0862de7c866c5bd7c32531f66738c21197af888
- https://git.kernel.org/stable/c/43683bb280330f3d36f0f2a3932a4867b9603e9c
- https://git.kernel.org/linus/d8e27d2d22b6e2df3a0125b8c08e9aace38c954c
- https://security-tracker.debian.org/tracker/CVE-2026-53085
- https://access.redhat.com/security/cve/CVE-2026-53085
- https://ubuntu.com/security/CVE-2026-53085

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53085
- https://bdu.fstec.ru/vul/2026-13989

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52969
BDU:2026-13927

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

Уязвимый продукт: Linux: от 6.19 до 7.0.9 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.

64

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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52969
- https://git.kernel.org/stable/c/74f1a22f7a80f03d28ad8551a2d25d563433addf
- https://git.kernel.org/stable/c/0eb281eb95b2d4eea4db1da5fe91023aecc97095
- https://git.kernel.org/stable/c/01b71b930f15728aa8599478a7ce90c19dcd9fc2
- https://git.kernel.org/stable/c/b315b033a877b1ee6d827810b5d7bb4392ffcf8d
- https://git.kernel.org/stable/c/0d419c23bb11b5c9664de777c47c1f04a235882d
- https://git.kernel.org/stable/c/ecf9b3ea7847fe14f34b8c41f00de1eb95c747da
- https://git.kernel.org/linus/577a8d3bae0531f0e5ccfac919cd8192f920a804
- https://security-tracker.debian.org/tracker/CVE-2026-52969

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52969
- https://ubuntu.com/security/CVE-2026-52969
- https://bdu.fstec.ru/vul/2026-13927

65

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53078
BDU:2026-13983

Идентификатор программной ошибки: CWE-126 Чтение за границей буфера

Уязвимый продукт: Linux: от 5.8.4 до 7.0.9 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: 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://www.cve.org/CVERecord?id=CVE-2026-53078
- https://git.kernel.org/stable/c/18e3ffde1822f0b48b1753bf34aa97ce839df1d8
- https://git.kernel.org/linus/10f86a2a5c91fc4c4d001960f1c21abe52545ef6
- https://security-tracker.debian.org/tracker/CVE-2026-53078
- https://access.redhat.com/security/cve/CVE-2026-53078
- https://ubuntu.com/security/CVE-2026-53078
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53078
- https://bdu.fstec.ru/vul/2026-13983

66

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53071
BDU:2026-13979

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 5.7 до 5.10.257 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 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: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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53071
- https://git.kernel.org/stable/c/96dca51715d86559ed6ed8028e5445cecb80f3ae
- https://git.kernel.org/stable/c/330b20ec97916961ee0e6c29c06bc0fa7c96e64c
- https://git.kernel.org/stable/c/0ccd75c51f620374086f359e906917676e699a1c
- https://git.kernel.org/stable/c/77a853aec710b2fdf41fa298ea3cbc9a4358f917
- https://git.kernel.org/stable/c/fe1188abdae9b7a8199dcdfcf9244d5e5d61eb14
- https://git.kernel.org/stable/c/dc89961b76f12aff47124c1df4bdb32a080f4d0c
- https://git.kernel.org/stable/c/5501d055a1ce3c747141e3955ba8cf034d193f3e

- https://git.kernel.org/linus/42776497cdbc9a665b384a6dcb85f0d4bd927eab
- https://security-tracker.debian.org/tracker/CVE-2026-53071
- https://access.redhat.com/security/cve/CVE-2026-53071
- https://ubuntu.com/security/CVE-2026-53071
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53071
- https://bdu.fstec.ru/vul/2026-13979

67

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53069
BDU:2026-13978

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 5.15 до 5.15.208 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53069
- https://git.kernel.org/stable/c/3128b294b426533c8d9162187446d93a8a160359
- https://git.kernel.org/stable/c/acbf45bd584d924b320bee2a7fe2a26f64904d95
- https://git.kernel.org/stable/c/866d3d9b87751b1944168fd82615505e0c0fd6cf
- https://git.kernel.org/stable/c/183128da0406b1c10e6f60b7b9fe70788b9c8c1d
- https://git.kernel.org/stable/c/7bad93e99737e4a5c0c14ac50c05152cf4e28022
- https://git.kernel.org/stable/c/ea690b3b6e58ae00979af8195b4cc24df466b65e
- https://git.kernel.org/linus/1921f91298d1388a0bb9db8f83800c998b649cb3

- https://security-tracker.debian.org/tracker/CVE-2026-53069
- https://access.redhat.com/security/cve/CVE-2026-53069
- https://ubuntu.com/security/CVE-2026-53069
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53069
- https://bdu.fstec.ru/vul/2026-13978

68

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53067
BDU:2026-13976

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

Уязвимый продукт: Linux: от 6.17 до 6.18.32 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53067
- https://git.kernel.org/stable/c/175717cfc06cab79f84cd037d66dda1b8564cd9e
- https://git.kernel.org/stable/c/3c25587fbf8797b92090b064a6d239a873e55fb1
- https://git.kernel.org/linus/1cba96c0a795124c3229293ed7b5b5765e66f259
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53067
- https://ubuntu.com/security/CVE-2026-53067
- https://bdu.fstec.ru/vul/2026-13976

69

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53055
BDU:2026-13973

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.17 до 6.18.32 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-2026-53055
- https://git.kernel.org/stable/c/b375c3c7209cc59e40e97998aa9bc768369cca0e
- https://git.kernel.org/stable/c/ad73563f3a1edbfddf2724136c6a15826b354e18
- https://git.kernel.org/linus/67b53a660e6bf0da2fa8d8872e897a14d8059eaf
- https://ubuntu.com/security/CVE-2026-53055
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53055
- https://bdu.fstec.ru/vul/2026-13973

70

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53054
BDU:2026-13972

Идентификатор программной ошибки: CWE-667 Некорректная блокировка

Уязвимый продукт: Linux: от 6.17 до 6.18.32 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: 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://www.cve.org/CVERecord?id=CVE-2026-53054
- https://git.kernel.org/stable/c/206f812ef140727b75697111391ae320fd8aa652
- https://git.kernel.org/stable/c/d9ecf758270501b2e7a0bc1dd69a6f28f1ae3cae
- https://git.kernel.org/linus/85042c2cd970a6b0e686329387096fe19989ae62
- https://ubuntu.com/security/CVE-2026-53054
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53054
- https://bdu.fstec.ru/vul/2026-13972

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53045
BDU:2026-13969

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: Linux: от 4.2 до 5.10.257 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

71

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-2026-53045
- https://git.kernel.org/stable/c/a85967331144fde9300be38bb44d2558eb6b742e
- https://git.kernel.org/stable/c/db0ae80865b515cc0b705c85877ec00f7eebe9fe
- https://git.kernel.org/stable/c/2369b1831161356e1bcb51385d3e532dc4fe2771
- https://git.kernel.org/stable/c/7e19e72f306484996c52ff96cc92f69b78ed5435
- https://git.kernel.org/stable/c/05f138fc7e27ee8e7a83ccf966c3fa26cda44dda
- https://git.kernel.org/stable/c/1793249c067a4b28e1aba0ad0e4d73aa9f9e165a
- https://git.kernel.org/stable/c/1ebbbef47d11cc90219c081492ccf995aaa3e9b3
- https://git.kernel.org/linus/9597ab9a8296ab337e6820f8a717ff621078b632

- https://security-tracker.debian.org/tracker/CVE-2026-53045
- https://ubuntu.com/security/CVE-2026-53045
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53045
- https://bdu.fstec.ru/vul/2026-13969

72

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53033
BDU:2026-13963

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.15 до 6.1.174 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 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: 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://www.cve.org/CVERecord?id=CVE-2026-53033
- https://git.kernel.org/stable/c/c6f4015eac2e3cbc3cb7a17539e10bbb5c2049c3
- https://git.kernel.org/stable/c/d0d124dbcef9318e326956137b31671407094bd4
- https://git.kernel.org/stable/c/1a59cc6b65fd3ad9915aae5970d859109d4ce9fb
- https://git.kernel.org/stable/c/921920c34cb591947dd30c692500795a69f1e3fa
- https://git.kernel.org/stable/c/98f744d204e5d6fca589cd2c44c3190a0c71697f
- https://git.kernel.org/linus/64c2f93fc3254d3bf5de4445fb732ee5c451edb6
- https://security-tracker.debian.org/tracker/CVE-2026-53033

- https://access.redhat.com/security/cve/CVE-2026-53033
- https://ubuntu.com/security/CVE-2026-53033
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53033
- https://bdu.fstec.ru/vul/2026-13963

73

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53031
BDU:2026-13961

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

Уязвимый продукт: Linux: от 6.9 до 6.12.90 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: 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://www.cve.org/CVERecord?id=CVE-2026-53031
- https://git.kernel.org/stable/c/31d3b4b28e55835646d6829d60023f730dd34e85
- https://git.kernel.org/stable/c/e15900888c09480a4c632bc598f1c5bd39bed6d6
- https://git.kernel.org/stable/c/fb66e20130f95a93ffea1677252526a9e39170b2
- https://git.kernel.org/linus/2845989f2ebaf7848e4eccf9a779daf3156ea0a5
- https://security-tracker.debian.org/tracker/CVE-2026-53031
- https://access.redhat.com/security/cve/CVE-2026-53031
- https://ubuntu.com/security/CVE-2026-53031

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53031
- https://bdu.fstec.ru/vul/2026-13961

74

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53081
BDU:2026-13986

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Linux: от 6.12 до 6.12.90 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: 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://www.cve.org/CVERecord?id=CVE-2026-53081
- https://git.kernel.org/stable/c/13c02881e49aac4c82b261faa26db9edf2567231
- https://git.kernel.org/stable/c/691adf738817275368ed56311b7d798d617823a3
- https://git.kernel.org/stable/c/7d73c72cccac651acc891377a5e623e4021c6380
- https://git.kernel.org/linus/2f2ec8e7730e21fc9bd49e0de9cdd58213ea24d0
- https://security-tracker.debian.org/tracker/CVE-2026-53081
- https://access.redhat.com/security/cve/CVE-2026-53081
- https://ubuntu.com/security/CVE-2026-53081

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53081
- https://bdu.fstec.ru/vul/2026-13986

75

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53016
BDU:2026-13954

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

Уязвимый продукт: Linux: от 3.14 до 5.10.257 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
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: 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://www.cve.org/CVERecord?id=CVE-2026-53016
- https://git.kernel.org/stable/c/939061b2d0f7f15114e34b4ce878ef50ff4089c3
- https://git.kernel.org/stable/c/798d409a8949f3f495f238549b86de2886b129bd
- https://git.kernel.org/stable/c/dfb2cf434829819268fe50f41542aad318ad62b2
- https://git.kernel.org/stable/c/eecee15e263ccb8cd77170a56ab6c969cb54dd6a
- https://git.kernel.org/stable/c/bb01d8f1f385bc9034ca114d3508c7fdea24fc9a
- https://git.kernel.org/stable/c/df9784bb5b637ac80f4a2768a58ca9a50bef28a9
- https://git.kernel.org/stable/c/227c1e1d9e2aa4cfc65ba446d5690da1f546cda4

- https://git.kernel.org/linus/a7a1f3cdd64d8a165d9b8c9e9ad7fb46ac19dfc4
- https://security-tracker.debian.org/tracker/CVE-2026-53016
- https://access.redhat.com/security/cve/CVE-2026-53016
- https://ubuntu.com/security/CVE-2026-53016
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53016
- https://bdu.fstec.ru/vul/2026-13954

76

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52976
BDU:2026-13931

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.12 до 6.12.90 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52976
- https://git.kernel.org/stable/c/f93b00161213a0fe9f7ff1d8498ee5ca9e0a5c43
- https://git.kernel.org/stable/c/753b149d5a433eb19e0c1b0eb4526a6e26120d1f
- https://git.kernel.org/stable/c/1be55646d8a2035343b012dcb12210db7bb8b056
- https://git.kernel.org/linus/f3cc22d4df3ed58439ea7e21daa54c3608e03b78
- https://security-tracker.debian.org/tracker/CVE-2026-52976
- https://access.redhat.com/security/cve/CVE-2026-52976
- https://ubuntu.com/security/CVE-2026-52976

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52976
- https://bdu.fstec.ru/vul/2026-13931

77

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53020
BDU:2026-13956

Идентификатор программной ошибки: CWE-414 Отсутствует проверка блокировки

Уязвимый продукт: Linux: от 6.19 до 7.0.9 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: 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://www.cve.org/CVERecord?id=CVE-2026-53020
- https://git.kernel.org/stable/c/f21c343ec7419377bff89ab11146c03ae117036f
- https://git.kernel.org/linus/102331b66bcaf1f41f50b9c4cd5c36e46bafa9f3
- https://ubuntu.com/security/CVE-2026-53020
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53020
- https://bdu.fstec.ru/vul/2026-13956

78

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52981
BDU:2026-13934

Идентификатор программной ошибки: CWE-772 Удержание ресурса после его использования

Уязвимый продукт: Linux: от 4.1 до 6.1.174 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52981
- https://git.kernel.org/stable/c/8a89054a1ec0767aec25ed2bbac933da6ba3cf5a
- https://git.kernel.org/stable/c/9247d59ca15bf60a57dca08103f055d8a4340877
- https://git.kernel.org/stable/c/0084712e0bee204b284510cdb63182fd5a30c2b7
- https://git.kernel.org/stable/c/63063ba60d2dc334e34f1e3f9271d7f3f6f30307
- https://git.kernel.org/stable/c/445e45a2c3a078316a62d2d331a570cf34ef5079
- https://git.kernel.org/linus/4438113be604ee67a7bf4f81da6e1cca41332ce4
- https://security-tracker.debian.org/tracker/CVE-2026-52981

- https://access.redhat.com/security/cve/CVE-2026-52981
- https://ubuntu.com/security/CVE-2026-52981
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52981
- https://bdu.fstec.ru/vul/2026-13934

79

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52989
BDU:2026-13939

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 6.18.10 до 6.18.32 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52989
- https://git.kernel.org/stable/c/3df42a854686fa06484e37ac1a3931c8e3e3453c
- https://git.kernel.org/stable/c/d7c8f95f599b3b38a717d2e771c3f8c174f657c3
- https://git.kernel.org/stable/c/f9204a2b78dd18374d3bcf9bf93d9021ce22de1b
- https://git.kernel.org/stable/c/c2a11441538bdbbc5aa003f190995eba93a89b88
- https://git.kernel.org/stable/c/046fa5c72d15cd8e2d592e275697ea399d8f76b0
- https://git.kernel.org/linus/ea8e356acb165cb1fd75537a52e1f66e5e76c538
- https://security-tracker.debian.org/tracker/CVE-2026-52989

- https://access.redhat.com/security/cve/CVE-2026-52989
- https://ubuntu.com/security/CVE-2026-52989
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52989
- https://bdu.fstec.ru/vul/2026-13939

80

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52991
BDU:2026-13940

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 5.2 до 6.18.32 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 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: 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://www.cve.org/CVERecord?id=CVE-2026-52991
- https://git.kernel.org/stable/c/03dc070fa0fc3cb4068693f468ccd5f8a7e58282
- https://git.kernel.org/stable/c/d4352c0709bfd38c752fccbde7fd72a82ac78f23
- https://git.kernel.org/linus/a5b98009f16d8a5fb4a8ff9a193f5735515c38fa
- https://security-tracker.debian.org/tracker/CVE-2026-52991
- https://access.redhat.com/security/cve/CVE-2026-52991
- https://ubuntu.com/security/CVE-2026-52991
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52991

- https://bdu.fstec.ru/vul/2026-13940

81

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52993
BDU:2026-13941

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

Уязвимый продукт: Linux: от 4.15 до 5.10.257 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-2026-52993
- https://git.kernel.org/stable/c/a438975a6dcdbd70865978c021650d1485586f0b
- https://git.kernel.org/stable/c/4ee4deadaae7cb2e3d53af0fc889cf92a73413c0
- https://git.kernel.org/stable/c/d3556656c6daebf8def751c7e71d11dd0a180d24
- https://git.kernel.org/stable/c/0274f24485fc38032d4093e463dc3ff5c7a667c9
- https://git.kernel.org/stable/c/4d104882bc815d4ec666ace9155f5f52715879a6
- https://git.kernel.org/stable/c/1d5e589055880fae229e229e1929e087dbe08cf3
- https://git.kernel.org/stable/c/29940fff14110ca48c5ccc168d121665b51bb778

- https://git.kernel.org/linus/d293ca716e7d5dffdaecaf6b9b2f857a33dc3d3a
- https://security-tracker.debian.org/tracker/CVE-2026-52993
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52993
- https://access.redhat.com/security/cve/CVE-2026-52993
- https://ubuntu.com/security/CVE-2026-52993
- https://bdu.fstec.ru/vul/2026-13941

82

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52998
BDU:2026-13943

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 2.6.31 до 5.10.257 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-52998
- https://git.kernel.org/stable/c/f4de0777e4554a7de19c920accde6319dd530782
- https://git.kernel.org/stable/c/c996a90f3071cf43683e5423da31aadbe002b8b4
- https://git.kernel.org/stable/c/edc806f9122961f0d3819f7c69c14cccde31f277
- https://git.kernel.org/stable/c/5d05de2f0928d81309a815ecc76d1a3ad72cbc16
- https://git.kernel.org/stable/c/95be653a76793856ff8b2d8bd82c2943c23f5ca8
- https://git.kernel.org/stable/c/79b90a96688e521771fa6ed3dc7864b76b8df293
- https://git.kernel.org/stable/c/83fc5dd63455a779ea2dd0f7ffee3c920919d80b

- https://git.kernel.org/linus/711987ba281fd806322a7cd244e98e2a81903114
- https://security-tracker.debian.org/tracker/CVE-2026-52998
- https://access.redhat.com/security/cve/CVE-2026-52998
- https://ubuntu.com/security/CVE-2026-52998
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52998
- https://bdu.fstec.ru/vul/2026-13943

83

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-52987
BDU:2026-13937

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

Уязвимый продукт: Linux: от 6.19 до 7.0.9 включительно
Red Hat Enterprise Linux: 10
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: 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://www.cve.org/CVERecord?id=CVE-2026-52987
- https://git.kernel.org/stable/c/c7c3ae7c01e5a0742b93cb9b40800bdd7f811e38
- https://git.kernel.org/linus/508babf310365f1107a2e8831c267c292a286818
- https://access.redhat.com/security/cve/CVE-2026-52987
- https://ubuntu.com/security/CVE-2026-52987
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52987
- https://bdu.fstec.ru/vul/2026-13937

84

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53000
BDU:2026-13945

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

Уязвимый продукт: Linux: от 5.14 до 6.18.32 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: 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53000
- https://git.kernel.org/stable/c/32fdd2e38e7435a368d88f5977a7d6585ebc8b0e
- https://git.kernel.org/stable/c/3c7511f38ab511b791196b13ae48bf4973bf7dfd
- https://git.kernel.org/linus/6eda0d771f94267f73f57c94630aa47e90957915
- https://security-tracker.debian.org/tracker/CVE-2026-53000
- https://access.redhat.com/security/cve/CVE-2026-53000
- https://ubuntu.com/security/CVE-2026-53000
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53000

- https://bdu.fstec.ru/vul/2026-13945

85

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53002
BDU:2026-13946

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.20 до 5.10.257 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-2026-53002
- https://git.kernel.org/stable/c/2f793ba78470a99f40389b7dc60a81d9f5ad3956
- https://git.kernel.org/stable/c/6bbf829b4c1b44c941c47dd0d710f1393258f3d5
- https://git.kernel.org/stable/c/ab64e61c9323fa6de21bd20da1ddb29a0fb65d34
- https://git.kernel.org/stable/c/1c9fb8aeed06790d42cdcd00f6c3ce0b9e926c1e
- https://git.kernel.org/stable/c/a8e0a32a23d3f34862af3b4da792ecb3a891a9a3
- https://git.kernel.org/stable/c/8e3be0d12615a173fe260cd42753ca7a001acbf2
- https://git.kernel.org/stable/c/c08ff52e44945e6ef4ce0790f49ea761b060c45b

- https://git.kernel.org/linus/6e7066bdb481a87fe88c4fa563e348c03b2d373d
- https://security-tracker.debian.org/tracker/CVE-2026-53002
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53002
- https://access.redhat.com/security/cve/CVE-2026-53002
- https://ubuntu.com/security/CVE-2026-53002
- https://bdu.fstec.ru/vul/2026-13946

86

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53004
BDU:2026-13947

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.24 до 5.10.257 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53004
- https://git.kernel.org/stable/c/a132e199de69e2a45628aa8534df1bf5d44e1b6e
- https://git.kernel.org/stable/c/2b5a2c957c7769d40110f725cf23987fcef50d75
- https://git.kernel.org/stable/c/d45c7e99caf915b0f6c716bd8ffe9d45b9685761
- https://git.kernel.org/stable/c/d67fbc6dea5dbf7f46c618ebf65910a276078e20
- https://git.kernel.org/stable/c/6849b995cda88a677bf08a05765d1db7905974fc
- https://git.kernel.org/stable/c/70a089cc9590aa347a61e84434116ab74619e3c3
- https://git.kernel.org/stable/c/6bcf8fe4ef7967b22b814cbae9a57bbd3c853410

- https://git.kernel.org/linus/0cf004ffb61cd32d140531c3a84afe975f9fc7ea
- https://security-tracker.debian.org/tracker/CVE-2026-53004
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53004
- https://access.redhat.com/security/cve/CVE-2026-53004
- https://ubuntu.com/security/CVE-2026-53004
- https://bdu.fstec.ru/vul/2026-13947

87

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53006
BDU:2026-13948

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.4 до 5.10.257 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: 2026-08-27 / 2026-08-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53006
- https://git.kernel.org/stable/c/7bff2c8fe5c35ae58bf73104f53db3676e6e5d94
- https://git.kernel.org/stable/c/aff0f28f5be803de2452ce702631c021fcd9ce8a
- https://git.kernel.org/stable/c/38bdbc897c0d83a3e2b925a51b69420f1feba29a
- https://git.kernel.org/stable/c/0069813e6ca9309eca78022bcb3aeb1e9ef90a12
- https://git.kernel.org/stable/c/1e1f0f89ee4692a64be3f3707ff8ac1ae57b03e7
- https://git.kernel.org/stable/c/7c66b368c6ff453f99cb39d84af93e908e51eef2
- https://git.kernel.org/stable/c/085e31a811ef234ef8c3e219c4636dfebfe7e10f

- https://git.kernel.org/linus/f996edd7615e686ada141b7f3395025729ff8ccb
- https://security-tracker.debian.org/tracker/CVE-2026-53006
- https://access.redhat.com/security/cve/CVE-2026-53006
- https://ubuntu.com/security/CVE-2026-53006
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53006
- https://bdu.fstec.ru/vul/2026-13948

88

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53009
BDU:2026-13949

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

Уязвимый продукт: Linux: от 4.17 до 6.6.140 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: 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: 2026-08-28 / 2026-08-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53009
- https://git.kernel.org/stable/c/4c08fc2119ef0281cfa2cee007acf0a251be55f2
- https://git.kernel.org/linus/1a303baa715e6b78d6a406aaf335f87ff35acfcd
- https://security-tracker.debian.org/tracker/CVE-2026-53009
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53009
- https://access.redhat.com/security/cve/CVE-2026-53009
- https://ubuntu.com/security/CVE-2026-53009
- https://bdu.fstec.ru/vul/2026-13949

89

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53011
BDU:2026-13950

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.2 до 5.10.257 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: 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://www.cve.org/CVERecord?id=CVE-2026-53011
- https://git.kernel.org/stable/c/a8fc396519ef4f081bc545e88f61241728bb78d7
- https://git.kernel.org/stable/c/3471874578160a28c171a607fa069f24062634b8
- https://git.kernel.org/stable/c/7256996e1ef553716817f3bfd077c2f3b48b582f
- https://git.kernel.org/stable/c/eee072fe16c646190d33ae69c9983d8de1562bf8
- https://git.kernel.org/stable/c/1bd286fa3e21200133478ed523cc6a2788baf38a
- https://git.kernel.org/stable/c/b73235da5dde77ed1264f9767b62c28c9d71fd78
- https://git.kernel.org/stable/c/0e62171df8ed4804d00db088f17eed06468233fa

- https://git.kernel.org/linus/105425b1969c5affe532713cfac1c0b320d7ac2b
- https://security-tracker.debian.org/tracker/CVE-2026-53011
- https://access.redhat.com/security/cve/CVE-2026-53011
- https://ubuntu.com/security/CVE-2026-53011
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53011
- https://bdu.fstec.ru/vul/2026-13950

90

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52999
BDU:2026-13944

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 4.20.13 до 5.10.257 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-2026-52999
- https://git.kernel.org/stable/c/0145548346c4a30981a870a8ca00eac46ba27e85
- https://git.kernel.org/stable/c/1c136f2c44a5913646bac85303612fd0825197a0
- https://git.kernel.org/stable/c/1e19a07291bb8682c14c39a64725a3ae54ab8ccc
- https://git.kernel.org/stable/c/32e50f92c7cf3f4eba29622179a5fcdc2aebab41
- https://git.kernel.org/stable/c/70a3f31d25cf2ec9d4ddfa408120171ead955623
- https://git.kernel.org/stable/c/21883587593d7c8bb519a79460a0b5bc5ffbdabd
- https://git.kernel.org/stable/c/edb78a142d2e5948e63647c0646aa7e7886935f0

- https://git.kernel.org/linus/f5ca450087c3baf3651055e7a6de92600f827af3
- https://security-tracker.debian.org/tracker/CVE-2026-52999
- https://access.redhat.com/security/cve/CVE-2026-52999
- https://ubuntu.com/security/CVE-2026-52999
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-52999
- https://bdu.fstec.ru/vul/2026-13944

91

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-45906
BDU:2026-14216

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.19 до 6.19.3 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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-45906
- https://git.kernel.org/stable/c/1bdefeed904f1f17e1f73a4d8a035515f3a9fad8
- https://git.kernel.org/linus/838767f5074700552d3f006d867caed65edc7328
- https://lore.kernel.org/linux-cve-announce/2026052721-CVE-2026-45906-7257@gregkh/
- https://bdu.fstec.ru/vul/2026-14216

92

Краткое описание: Выполнение произвольного кода в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-19490
BDU:2026-14208

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: NetScaler Gateway: от 13.1 до 63.21
NetScaler ADC: от 13.1 до 63.21

Категория уязвимого продукта: Серверное программное обеспечение и его 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.

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: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939
- https://github.com/TarPeg007/CVE-2026-19490
- https://bdu.fstec.ru/vul/2026-14208

93

Краткое описание: Выполнение произвольного кода в Composer

Идентификатор уязвимости: CVE-2026-84361
BDU:2026-14209

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Composer: от 1.0 до 2.2.30

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: 7.5 AV:N/AC:H/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://github.com/Saku0512/CVE-2026-84361-poc
- https://github.com/composer/composer/commit/0aac50528e83ed635cf788333635897469440220
- https://github.com/composer/composer/commit/199ad81a9cc6a2a5164ad79a8da26b2e19e521af
- https://github.com/composer/composer/releases/tag/2.10.3
- https://github.com/composer/composer/releases/tag/2.2.30
- https://github.com/composer/composer/security/advisories/GHSA-rvx4-ffvw-m9q3
- https://bdu.fstec.ru/vul/2026-14209

94

Краткое описание: Повышение привилегий в Python NLTK library

Идентификатор уязвимости: CVE-2026-12841
BDU:2026-14210

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: NLTK: до 3.10.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

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: 2026-09-04 / 2026-09-04

Ссылки на источник:

- https://dailycve.com/nltk-stanford-wrappers-jvm-argument-injection-bypass-cve-2026-12841-critical-dc-sep2026-2068/
- https://github.com/advisories/GHSA-m4rf-3fr8-xwx3
- https://bdu.fstec.ru/vul/2026-14210

95

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46039
BDU:2026-14213

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

Уязвимый продукт: Linux: от 6.16.9 до 6.18.26 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: 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://www.cve.org/CVERecord?id=CVE-2026-46039
- https://git.kernel.org/stable/c/43222ac484f93b3ec2d240a7575e1cedd31f5fa4
- https://git.kernel.org/stable/c/183d37f12d1c8ed24a5bfc7addad05510da22a94
- https://git.kernel.org/linus/6929350080f4da292d111a3b33e53138fee51cec
- https://lore.kernel.org/linux-cve-announce/2026052751-CVE-2026-46039-e5c2@gregkh/
- https://bdu.fstec.ru/vul/2026-14213

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46075
BDU:2026-14217

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 5.3 до 6.1.174 включительно
Red Hat Enterprise Linux: 10
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.

96

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46075
- https://git.kernel.org/stable/c/c5a45d14234bf26e28a89e3a5dcc08336595cf11
- https://git.kernel.org/stable/c/775c00d87c385b758da9504cf053acea00e2ed40
- https://git.kernel.org/stable/c/1193c12126d39bf986a5a9214827b73707b193ab
- https://git.kernel.org/stable/c/31901371ccd16b42d2f167b1018ba9ae8bd5a6c7
- https://git.kernel.org/linus/bab1adf3b87e4bfac92c4f5963c63db434d561c1
- https://lore.kernel.org/linux-cve-announce/2026052759-CVE-2026-46075-8a6c@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46075
- https://access.redhat.com/security/cve/cve-2026-46075

- https://bdu.fstec.ru/vul/2026-14217

97

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46205
BDU:2026-14224

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Linux: от 4.12 до 5.10.257 включительно
Debian GNU/Linux: 13

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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46205
- https://git.kernel.org/stable/c/8c7a281a99224a5b9af99c4dcd98d68eea75926c
- https://git.kernel.org/stable/c/6f1ce75a75c65061e7a720c3d0ee5f8adab7a2d3
- https://git.kernel.org/stable/c/c7848b67ef10f581114b6a2f52b160fc20eb52c9
- https://git.kernel.org/stable/c/6850a439f8d23d4979624f1d6880d3118d473a28
- https://git.kernel.org/linus/2b7eb2c5dc72f0fc954ac4aa155f9e285e937f7c
- https://lore.kernel.org/linux-cve-announce/2026052833-CVE-2026-46205-24bf@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46205
- https://bdu.fstec.ru/vul/2026-14224

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46115
BDU:2026-14219

Идентификатор программной ошибки: CWE-372 Некорректное определение внутреннего состояния

Уязвимый продукт: Linux: от 6.7 до 6.12.87 включительно
Red Hat Enterprise Linux: 10
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.

98

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://www.cve.org/CVERecord?id=CVE-2026-46115
- https://git.kernel.org/stable/c/3d2ecbd444b01d6500671d1a582b7393943cf539
- https://git.kernel.org/stable/c/a7f3aa8c9df3905fe820ae36b67ba56b81587574
- https://git.kernel.org/stable/c/f17d521075325b8afc42d1baa1c28a5e9aca111f
- https://git.kernel.org/stable/c/f632dab4b841554cd6416058c61886d7db176581
- https://git.kernel.org/linus/13920e4b7b784b40cf4519ff1f0f3e513476a499
- https://lore.kernel.org/linux-cve-announce/2026052813-CVE-2026-46115-6be3@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46115
- https://access.redhat.com/security/cve/cve-2026-46115

- https://bdu.fstec.ru/vul/2026-14219

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46120
BDU:2026-14220

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

Уязвимый продукт: Linux: от 4.16.12 до 5.10.257 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Debian GNU/Linux: 13

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.

99

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46120
- https://git.kernel.org/stable/c/eca62bb0569de4d43a4dac06a2092a9d4ca1d702
- https://git.kernel.org/stable/c/311fdd26eb4443d43b909cc67a10f3a5fd1b21b2
- https://git.kernel.org/stable/c/e70cfb40c3a99b232cd42c6a6a10f0d8e039dc82
- https://git.kernel.org/stable/c/cf7fc624329e76c6394653d12353e1d033adea91
- https://git.kernel.org/linus/1d324c2f43f70c965f25c58cc3611c779adbe47e
- https://lore.kernel.org/linux-cve-announce/2026052815-CVE-2026-46120-1a01@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46120
- https://access.redhat.com/security/cve/cve-2026-46120

- https://bdu.fstec.ru/vul/2026-14220

100

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-45929
BDU:2026-14221

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.16 до 6.18.13 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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-45929
- https://git.kernel.org/stable/c/3e4fbcb4e078915367ba5576cd70d76dbc970f95
- https://git.kernel.org/stable/c/442915c96a9bff1c7080e2aedabb1c03faa28d81
- https://git.kernel.org/linus/a5ec7baa44ea3a1d6aa0ca31c0ad82edf9affe41
- https://bdu.fstec.ru/vul/2026-14221

101

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46053
BDU:2026-14222

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

Уязвимый продукт: Linux: от 5.6 до 5.10.257 включительно
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: 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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46053
- https://git.kernel.org/stable/c/8fdbb6262a4a3ed44a0830a7793903b54bb27bdc
- https://git.kernel.org/stable/c/d95cea9298be1ba8876e3f156be96d3a492085ca
- https://git.kernel.org/stable/c/033370ffb3c9c0264d19f8ba9ef769523266589a
- https://git.kernel.org/stable/c/b3cb8cae530b2727d8245684148bb49425f6765c
- https://git.kernel.org/linus/8141a2dc70080eda1aedc0389ed2db2b292af5bd
- https://lore.kernel.org/linux-cve-announce/2026052754-CVE-2026-46053-a24e@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46053
- https://bdu.fstec.ru/vul/2026-14222

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46209
BDU:2026-14223

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

Уязвимый продукт: Linux: от 4.14 до 5.10.257 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
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.

102

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46209
- https://git.kernel.org/stable/c/6b992591e04f2cce813bcf239b354f375bbf84d3
- https://git.kernel.org/stable/c/1da4ab7189f1064b3b712b388772c008b4d82580
- https://git.kernel.org/stable/c/1a17ea9861e89585361caa8bc231bd22dc6dbe7d
- https://git.kernel.org/stable/c/c5fc49d8470c5ebf3b41607600f277158f159950
- https://git.kernel.org/linus/3d4c2268bd7243c3780fe32bf24ff876da272acf
- https://lore.kernel.org/linux-cve-announce/2026052834-CVE-2026-46209-e4e9@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46209
- https://access.redhat.com/security/cve/cve-2026-46209

- https://bdu.fstec.ru/vul/2026-14223

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46201
BDU:2026-14225

Идентификатор программной ошибки: CWE-772 Удержание ресурса после его использования

Уязвимый продукт: Linux: от 6.8 до 6.12.89 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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.

103

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46201
- https://git.kernel.org/stable/c/d394669e194936d7ce15284a24a5ae334c4c5b74
- https://git.kernel.org/stable/c/0afa8b1ef582ecf6fb04097fd356f8741e5005ed
- https://git.kernel.org/stable/c/eea1e10f8d99c0f04deef707c99705b94bba3b78
- https://git.kernel.org/linus/111ab678471bf1f90d078d5513bb086b70596c3c
- https://lore.kernel.org/linux-cve-announce/2026052832-CVE-2026-46201-2126@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46201
- https://access.redhat.com/security/cve/cve-2026-46201
- https://bdu.fstec.ru/vul/2026-14225

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46173
BDU:2026-14226

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

Уязвимый продукт: Linux: от 5.17 до 6.1.174 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
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.

104 **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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46173
- https://git.kernel.org/stable/c/640b4c00fb0e2920327435f6176cbefc3c546165
- https://git.kernel.org/stable/c/7b2800ba5f5f77a8ee7f4cbadb19cf1264597a34
- https://git.kernel.org/stable/c/6f49f94f3b11fe8bff1bf2a054143789e76aaf17
- https://git.kernel.org/stable/c/9756b3db5db6c2f5eccb32dddbd88eb4c54f575e
- https://git.kernel.org/linus/c1fa0bb633e4a6b11e83ffc57fa5abe8ebb87891
- https://lore.kernel.org/linux-cve-announce/2026052827-CVE-2026-46173-0214@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46173.:
- https://access.redhat.com/security/cve/cve-2026-46173

- https://bdu.fstec.ru/vul/2026-14226

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46081
BDU:2026-14227

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

Уязвимый продукт: Linux: от 6.16 до 6.18.26 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.

105

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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46081
- https://git.kernel.org/stable/c/343a5bf68a8ff9affcf2b70677ea4cf40c195ee4
- https://git.kernel.org/stable/c/1a2785e5985627f2265ba7775949601a29ba0d1e
- https://git.kernel.org/linus/d7e20b9bd6c990773cf0c09e2642250b8a70263d
- https://lore.kernel.org/linux-cve-announce/2026052700-CVE-2026-46081-dd38@gregkh/
- https://bdu.fstec.ru/vul/2026-14227

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46241
BDU:2026-14218

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.33 до 6.12.89 включительно
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.

106 **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: 2026-08-25 / 2026-08-25

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-46241
- https://git.kernel.org/stable/c/8b49b6aadd0c622ca7d68b4a53ae10362e221cf3
- https://git.kernel.org/stable/c/336d9ad7560b3baba17af06727a888040ee93390
- https://git.kernel.org/stable/c/5c77f11b9b5f1ad5a704dad875260c44016ede10
- https://git.kernel.org/linus/f62c060272b9d7423b1650b844e8e4e7b8f9f925
- https://lore.kernel.org/linux-cve-announce/2026052842-CVE-2026-46241-679a@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-46241
- https://bdu.fstec.ru/vul/2026-14218

107

Краткое описание: Межсайтовый скриптинг в SIMATIC S7 PLC

Идентификатор уязвимости: CVE-2026-25786
BDU:2026-14204

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: SIMATIC ET 200SP Open Controller CPU 1515SP PC: -
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK: -
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK: -
SIMATIC S7-PLCSIM Advanced: -
SIMATIC Drive Controller CPU 1504D TF: до 3.1.6
SIMATIC Drive Controller CPU 1507D TF: до 3.1.6
SIMATIC S7-1500 CPU 1511-1 PN: до 3.1.4
SIMATIC S7-1500 CPU 1511C-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1511F-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1511T-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1511TF-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1512C-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1513-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1513F-1 PN: до 2.9.9
SIMATIC S7-1500 CPU 1515-2 PN: до 2.9.9
SIMATIC S7-1500 CPU 1515F-2 PN: до 2.9.9
SIMATIC S7-1500 CPU 1515T-2 PN: до 2.9.9
SIMATIC S7-1500 CPU 1515TF-2 PN: до 2.9.9
SIMATIC S7-1500 CPU 1516-3 PN/DP: до 2.9.9
SIMATIC S7-1500 CPU 1516F-3 PN/DP: до 2.9.9
SIMATIC S7-1500 CPU 1516T-3 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1517-3 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1517F-3 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1517TF-3 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1518-4 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP: до 3.1.6
SIMATIC S7-1500 CPU 1518T-4 PN/DP: до 3.1.6
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN: до 2.9.9

SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN: до 2.9.9
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN: до 2.9.9
SIPLUS ET 200SP CPU 1510SP F-1 PN: до 2.9.9
SIPLUS ET 200SP CPU 1510SP-1 PN: до 2.9.9
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL: до 2.9.9
SIPLUS ET 200SP CPU 1512SP F-1 PN: до 2.9.9
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL: до 2.9.9
SIPLUS ET 200SP CPU 1512SP-1 PN: до 2.9.9
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1511-1 PN: до 2.9.9
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1511F-1 PN: до 2.9.9
SIPLUS S7-1500 CPU 1513-1 PN: до 2.9.9
SIPLUS S7-1500 CPU 1513F-1 PN: до 2.9.9
SIPLUS S7-1500 CPU 1515F-2 PN: до 2.9.9
SIPLUS S7-1500 CPU 1515F-2 PN RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1516-3 PN/DP: до 2.9.9
SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1516F-3 PN/DP: до 2.9.9
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL: до 2.9.9
SIPLUS S7-1500 CPU 1518-4 PN/DP: до 3.1.6
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP: до 3.1.6
SIPLUS S7-1500 CPU 1518F-4 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP: до 3.1.6
SIMATIC S7-1500 CPU 1518F-4 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1518TF-4 PN/DP: до 3.1.6
SIMATIC S7-1500 CPU 1516TF-3 PN/DP: -
SIMATIC S7-1500 CPU 1513pro F-2 PN: -
SIMATIC S7-1500 CPU 1513pro-2 PN: -
SIMATIC S7-1500 CPU 1516pro F-2 PN: -
SIMATIC S7-1500 CPU 1516pro-2 PN: -

SIMATIC ET 200SP CPU 1510SP F-1 PN: до 2.9.9
SIMATIC ET 200SP CPU 1510SP-1 PN: до 2.9.9
SIMATIC ET 200SP CPU 1512SP F-1 PN: до 2.9.9
SIMATIC ET 200SP CPU 1512SP-1 PN: до 2.9.9
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V2 CPUs: -
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs: -
SIMATIC ET 200SP Open Controller CPU 1515SP PC3 V4 CPUs: -
SIMATIC ET 200SP CPU 1514SP F-2 PN: -
SIMATIC ET 200SP CPU 1514SP-2 PN: -
SIMATIC ET 200SP CPU 1514SPT F-2 PN: -
SIMATIC ET 200SP CPU 1514SPT-2 PN: -
SIMATIC S7-1500 CPU 1517T-3 PN/DP: -
SIMATIC S7-1500 CPU 1518-3 PN: -
SIMATIC S7-1500 CPU 1518F-3 PN: -
SIMATIC S7-1500 CPU 1518T-3 PN: -
SIMATIC S7-1500 CPU 1518TF-3 PN: -
SIMATIC S7-1500 Software Controller CPU 1507S F V2: -
SIMATIC S7-1500 Software Controller CPU 1508S F V2: -
SIMATIC S7-1500 Software Controller Linux V2: -
SIMATIC S7-1500 Software Controller CPU 1507S F V3: -
SIMATIC S7-1500 Software Controller CPU 1508S F V3: -
SIMATIC S7-1500 Software Controller CPU 1508S T V3: -
SIMATIC S7-1500 Software Controller CPU 1508S TF V3: -
SIMATIC S7-1500 Software Controller CPU 1508S V3: -
SIMATIC S7-1500 Software Controller Linux V3: -
SIMATIC S7-1500 Software Controller CPU 1507S F V4: -
SIMATIC S7-1500 Software Controller CPU 1507S V4: -
SIMATIC S7-1500 Software Controller CPU 1508S F V4: -
SIMATIC S7-1500 Software Controller CPU 1508S V4: -

Категория уязвимого продукта: Программно-аппаратное решение

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: 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-688146.html
- https://bdu.fstec.ru/vul/2026-14204

108

Краткое описание: Повышение привилегий в SIMATIC HMI Unified Comfort

Идентификатор уязвимости: CVE-2026-27662
BDU:2026-14203

Идентификатор программной ошибки: CWE-1005 Отображение и проверка входных данных

Уязвимый продукт: SIMATIC HMI MTP700 Unified Comfort Panel hygienic neutral design: до 21
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic: до 21
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic neutral design: до 21
SIMATIC HMI MTP1200 Unified Comfort Panel hygienic: до 21
SIMATIC HMI MTP1200 Unified Comfort Panel hygienic neutral design: до 21
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic: до 21
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic neutral design: до 21
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic: до 21
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic neutral design: до 21
SIMATIC HMI MTP2200 Unified Comfort Hygienic: до 21
SIMATIC HMI MTP2200 Unified Comfort Hygienic neutral design: до 21
SIMATIC HMI MTP700 Unified Comfort Panel neutral design: до 21
SIMATIC HMI MTP700 Unified Comfort Panel: до 21
SIMATIC HMI MTP1000 Unified Comfort Panel: до 21
SIMATIC HMI MTP1000 Unified Comfort Panel neutral: до 21
SIMATIC HMI MTP1200 Comfort Pro for stand: до 21
SIMATIC HMI MTP1200 Comfort Pro for support arm: до 21
SIMATIC HMI MTP1200 Comfort Pro neutral design for stand: до 21
SIMATIC HMI MTP1200 Comfort Pro neutral design for support arm: до 21
SIMATIC HMI MTP1200 Unified Comfort Panel: до 21
SIMATIC HMI MTP1200 Unified Comfort Panel neutral design: до 21
SIMATIC HMI MTP1500 Comfort Pro for stand: до 21
SIMATIC HMI MTP1500 Comfort Pro for support arm: до 21
SIMATIC HMI MTP1500 Comfort Pro neutral design for stand: до 21
SIMATIC HMI MTP1500 Comfort Pro neutral design for support arm: до 21
SIMATIC HMI MTP1500 Unified Comfort Panel: до 21
SIMATIC HMI MTP1500 Unified Comfort Panel neutral design: до 21
SIMATIC HMI MTP1900 Comfort Pro for stand: до 21
SIMATIC HMI MTP1900 Comfort Pro for support arm: до 21

SIMATIC HMI MTP1900 Comfort Pro neutral design for stand: до 21
SIMATIC HMI MTP1900 Comfort Pro neutral design for support arm: до 21
SIMATIC HMI MTP1900 Unified Comfort Panel: до 21
SIMATIC HMI MTP1900 Unified Comfort Panel neutral design: до 21
SIMATIC HMI MTP2200 Comfort Pro for stand: до 21
SIMATIC HMI MTP2200 Comfort Pro for support arm: до 21
SIMATIC HMI MTP2200 Comfort Pro neutral design for stand: до 21
SIMATIC HMI MTP2200 Comfort Pro neutral design for support arm: до 21
SIMATIC HMI MTP2200 Unified Comfort Panel: до 21
SIMATIC HMI MTP2200 Unified Comfort Panel neutral design: до 21
SIPLUS HMI MTP700 Unified Comfort: до 21
SIPLUS HMI MTP1000 Unified Comfort: до 21
SIPLUS HMI MTP1200 Unified Comfort: до 21

Категория уязвимого продукта: Программно-аппаратное решение

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: 7.7 AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

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-387223.html
- https://bdu.fstec.ru/vul/2026-14203

Краткое описание: Повышение привилегий в Util-linux

Идентификатор уязвимости: CVE-2026-76642
BDU:2026-14159

Идентификатор программной ошибки: CWE-390 Обнаружение ошибки без реагирования на нее

Уязвимый продукт: util-linux: до 2.42.2 включительно

Категория уязвимого продукта: Unix-подобные операционные системы 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.

109

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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://github.com/util-linux/util-linux/blob/v2.42.2/libmount/src/context_mount.c#L476
- https://github.com/util-linux/util-linux/blob/v2.42.2/libmount/src/context_mount.c#L892
- https://github.com/util-linux/util-linux/commit/1d14676ea70003e9f5b2a6a76af0cadb1190411a
- https://github.com/util-linux/util-linux/commit/a15c00a9e545aa8b9cf6ec0f888ff6c7b3eaeedc
- https://github.com/util-linux/util-linux/commit/f57cea130839c0af8dc0525274267ae4cfd66bbf
- https://github.com/util-linux/util-linux/security/advisories/GHSA-m25x-3hj9-m26f
- https://bdu.fstec.ru/vul/2026-14159

Краткое описание: Выполнение произвольного кода в LibTIFF

Идентификатор уязвимости: CVE-2026-52490
BDU:2026-14164

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

Уязвимый продукт: LibTIFF: 4.7.1

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.

110

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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://gist.github.com/okyfh/122c2d72e991a78c8af80a3af3be8671
- https://gitlab.com/libtiff/libtiff/-/commit/627f9f526f1c0fb2d8e4fb2b2c8e8234413b9003
- https://gitlab.com/libtiff/libtiff/-/work_items/846
- https://bdu.fstec.ru/vul/2026-14164

111

Краткое описание: Выполнение произвольного кода в FortiClient Windows

Идентификатор уязвимости: CVE-2026-70465
BDU:2026-14167

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: FortiClient Windows: от 7.2.0 до 7.2.12

Категория уязвимого продукта: Средства защиты информации

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: 2026-08-26 / 2026-08-26

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-156
- https://bdu.fstec.ru/vul/2026-14167

112

Краткое описание: Обход безопасности в Prisma Access Agent

Идентификатор уязвимости: CVE-2026-0292
BDU:2026-14183

Идентификатор программной ошибки: CWE-290 Обход аутентификации, связанный с подменой данных

Уязвимый продукт: Prisma Access Agent: до 26.3

Категория уязвимого продукта: Прикладное программное обеспечение

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: 8.4 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: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0292
- https://www.tenable.com/cve/CVE-2026-0292
- https://bdu.fstec.ru/vul/2026-14183

113

Краткое описание: Повышение привилегий в Prisma Access Agent

Идентификатор уязвимости: CVE-2026-0294
BDU:2026-14184

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Prisma Access Agent: до 26.3

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0294
- https://www.tenable.com/cve/CVE-2026-0294
- https://bdu.fstec.ru/vul/2026-14184

114

Краткое описание: Выполнение произвольного кода в GlobalProtect App

Идентификатор уязвимости: CVE-2026-0297
BDU:2026-14187

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: GlobalProtect App: от 6.0.0 до 6.0.15

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: 8.1 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://security.paloaltonetworks.com/CVE-2026-0297
- https://www.tenable.com/cve/CVE-2026-0297
- https://bdu.fstec.ru/vul/2026-14187

115

Краткое описание: Повышение привилегий в GlobalProtect App

Идентификатор уязвимости: CVE-2026-0299
BDU:2026-14189

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: GlobalProtect App: от 6.0.0 до 6.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0299
- https://www.tenable.com/cve/CVE-2026-0299
- https://bdu.fstec.ru/vul/2026-14189

116

Краткое описание: Получение конфиденциальной информации в PAN-OS

Идентификатор уязвимости: CVE-2026-0301
BDU:2026-14190

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: PAN-OS: от 11.1.0 до 11.1.16-h1
Prisma Access: от 10.2.0 до 10.2.10
Cloud NGFW: -

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 2026-08-24 / 2026-08-24

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0301
- https://www.tenable.com/cve/CVE-2026-0301
- https://bdu.fstec.ru/vul/2026-14190

117

Краткое описание: Перезапись произвольных файлов в ThinManager

Идентификатор уязвимости: CVE-2026-11917
BDU:2026-14199

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

Уязвимый продукт: ThinManager: от 14.0.0 до 14.0.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 8.1 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1782.html
- https://bdu.fstec.ru/vul/2026-14199

118

Краткое описание: Отказ в обслуживании в Prisma Access Agent

Идентификатор уязвимости: CVE-2026-0291
BDU:2026-14181

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Prisma Access Agent: до 26.2.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Злоупотребление функционалом.

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: 2026-08-21 / 2026-08-21

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0291
- https://www.tenable.com/cve/CVE-2026-0291
- https://bdu.fstec.ru/vul/2026-14181

119

Краткое описание: Получение конфиденциальной информации в phpMyFAQ

Идентификатор уязвимости: CVE-2026-85591
BDU:2026-14240

Идентификатор программной ошибки: CWE-620 Смена пароля без подтверждения

Уязвимый продукт: phpMyFAQ: до 4.1.8

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

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: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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-6r2c-694w-24qv
- https://bdu.fstec.ru/vul/2026-14240

120

Краткое описание: Повышение привилегий в Cleo Harmony

Идентификатор уязвимости: CVE-2026-84115
BDU:2026-14239

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Cleo Harmony: от 5.8.1.0 до 5.8.1.10 включительно

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: 8.3 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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://t.me/ZerodayAlert/823
- https://support.cleo.com/hc/en-us/articles/30258468834583-Cleo-Harmony-5-8-1-Release-Notes#Version58111
- https://www.securitylab.ru/news/576903.php
- https://365trust.me/cleo-harmony-disponibile-poc-per-la-cve-2026-84115-al04-260903-csirt-ita/
- https://bdu.fstec.ru/vul/2026-14239

121

Краткое описание: Отказ в обслуживании в Open5GS

Идентификатор уязвимости: CVE-2026-75438
BDU:2026-14236

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Open5GS: до 2.8.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://github.com/hackeryounow/5GCVulDB/tree/main/CVE-2026-75438
- https://github.com/open5gs/open5gs/issues/4612
- https://github.com/open5gs/open5gs/commit/7227b2f5b254160286798e058c189224360d99fc
- https://gist.github.com/hackeryounow/c299d593b89fd6487cab4182c8aecabf
- https://bdu.fstec.ru/vul/2026-14236

122

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-64563
BDU:2026-14233

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 7.1.6
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-64563
- https://security-tracker.debian.org/tracker/CVE-2026-64563
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64563
- https://git.kernel.org/linus/8173f7e2ce67e6ca1d4763f3da14e5b01ce77456
- https://git.kernel.org/stable/c/3ff7c1dbf722cf3fa538672452ba182318e0fcc3
- https://git.kernel.org/stable/c/4169d9fb92f313ff8e7e83d733c1ecdcc93eebd3
- https://git.kernel.org/stable/c/8173f7e2ce67e6ca1d4763f3da14e5b01ce77456

- https://github.com/nebusecurity/security-research/tree/rhashtable/pocs/linux/kernelctf/CVE-2026-64563_lts
- https://lore.kernel.org/linux-cve-announce/2026080404-CVE-2026-64563-9d7f@gregkh/T/#u
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0903SE18HF
- https://ubuntu.com/security/CVE-2026-64563
- https://access.redhat.com/security/cve/CVE-2026-64563
- https://bdu.fstec.ru/vul/2026-14233

123

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53264
BDU:2026-14230

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 4.14 до 5.10.259
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-53264
- https://security-tracker.debian.org/tracker/CVE-2026-53264
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53264
- https://git.kernel.org/linus/5057e1aca011e51ef51498c940ef96f3d3e8a305
- https://git.kernel.org/stable/c/18af5d2ef0c4f65787fd1280c8b23286b9f2a835
- https://git.kernel.org/stable/c/1f1b98fea6b9ea30507d0f2fbff6750292d097e2
- https://git.kernel.org/stable/c/5057e1aca011e51ef51498c940ef96f3d3e8a305

- https://git.kernel.org/stable/c/5dd51e09020c65aa53cf128e5e3517cd53b3c113
- https://git.kernel.org/stable/c/8b136f18ac4b2ace5aaad3305b3f8a5d8165a009
- https://git.kernel.org/stable/c/91d105d2cbe002f9c7b43a6183adedc37e1da1f7
- https://git.kernel.org/stable/c/98b2e40879abf0245be5a5b7af69e0f6ff524ac3
- https://git.kernel.org/stable/c/b60e9391142e983fab2be53497aa8f71fdd09cd5
- https://github.com/star-sg/CVE/tree/master/CVE-2026-53264
- https://lore.kernel.org/linux-cve-announce/2026062517-CVE-2026-53264-081f@gregkh/T
- https://starlabs.sg/blog/2026/07-when-ai-makes-0-days-feel-like-n-days/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0903SE18HF
- https://ubuntu.com/security/CVE-2026-53264
- https://access.redhat.com/security/cve/CVE-2026-53264
- https://bdu.fstec.ru/vul/2026-14230

124

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64076
BDU:2026-14405

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 5.13 до 6.18.33 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 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64076
- https://git.kernel.org/linus/27414ff1b287ea9a2a11675149ec28e05539f3cc
- https://git.kernel.org/stable/c/c647e2a21bbbaceda6cdb8a44a56f44d231dc4b4
- https://git.kernel.org/stable/c/02d999dc69b3918dba2414932b5d95f1f75c76cb
- https://security-tracker.debian.org/tracker/CVE-2026-64076
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64076
- https://access.redhat.com/security/cve/CVE-2026-64076
- https://ubuntu.com/security/CVE-2026-64076

- https://bdu.fstec.ru/vul/2026-14405

125

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63911
BDU:2026-14404

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

Уязвимый продукт: Linux: от 6.14 до 6.18.34 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63911
- https://git.kernel.org/linus/7f83d174073234839aea176f265e517e0d50a1d2
- https://git.kernel.org/stable/c/9327252e04626d4bb02ca8c0c108fbe8eabf0c5a
- https://git.kernel.org/stable/c/dfb9f6cbfa9826655a49698cf90eb800fce2178e
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63911
- https://ubuntu.com/security/CVE-2026-63911
- https://bdu.fstec.ru/vul/2026-14404

126

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63875
BDU:2026-14403

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.18.13 до 6.18.34 включительно
Red Hat Enterprise Linux: 9
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63875
- https://git.kernel.org/linus/c2ff4764e03e7a8d758352f4aceb8fe1be6ac971
- https://git.kernel.org/stable/c/dced308d7d6a0de1c09d2058f38f1aaaf5cbb914
- https://git.kernel.org/stable/c/47490bbb05c8c0e09cc3cfd237d8934ffc340583
- https://git.kernel.org/stable/c/0199c9d57861f17b556b6cba1f765c7cce79745b
- https://git.kernel.org/stable/c/d766a49d9b55705c4737cd8bb5d3faa2d31330fd
- https://git.kernel.org/stable/c/8ca7284da0e67b3e71d90ec17f08286774245ad9
- https://git.kernel.org/stable/c/fe93e907b1af03cc229a80aa64a570a103d2b279

- https://git.kernel.org/stable/c/48125cd9c55cbe297b59fd1f9bda48b0960bd181
- https://security-tracker.debian.org/tracker/CVE-2026-63875
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63875
- https://access.redhat.com/security/cve/CVE-2026-63875
- https://ubuntu.com/security/CVE-2026-63875
- https://bdu.fstec.ru/vul/2026-14403

127

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63879
BDU:2026-14402

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Linux: от 6.2 до 7.0.11 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63879
- https://git.kernel.org/linus/962d684b5dc0741dcd93485d41b450de402d5592
- https://git.kernel.org/stable/c/2fd24407457a6b181ba827705678da70e528dcd0
- https://security-tracker.debian.org/tracker/CVE-2026-63879
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63879
- https://access.redhat.com/security/cve/CVE-2026-63879
- https://ubuntu.com/security/CVE-2026-63879
- https://bdu.fstec.ru/vul/2026-14402

128

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64046
BDU:2026-14401

Идентификатор программной ошибки: CWE-237 Некорректная обработка структурных элементов

Уязвимый продукт: Linux: от 5.4.14 до 5.10.257 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64046
- https://git.kernel.org/linus/ff26a0e8377dec07e4a7230db7675bed1b9a6d03
- https://git.kernel.org/stable/c/49a5faaa471ddcd37b6893970c9916eb836e7c31
- https://git.kernel.org/stable/c/91359966e247c0244c66d50bbb8e74aefa4321c3
- https://git.kernel.org/stable/c/410351158dfef2d67fea6603680b3a6013c6ed9d
- https://git.kernel.org/stable/c/acdc12b71c9aa4be5dcd2c8062753c6d2033e235
- https://git.kernel.org/stable/c/929b1548e63ac72e104c07d8ee8cbbeeba2fa89a
- https://git.kernel.org/stable/c/af855f4c966afafef74faf8390c7b86568c0d46d

- https://git.kernel.org/stable/c/b9c015ef1a7bf1e8dc67f21c6381f36deb2c3a36
- https://ubuntu.com/security/notices/USN-8575-1
- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-64046
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64046
- https://access.redhat.com/security/cve/CVE-2026-64046
- https://ubuntu.com/security/CVE-2026-64046
- https://bdu.fstec.ru/vul/2026-14401

129

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63888
BDU:2026-14400

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 3.1 до 5.10.258 включительно
Red Hat Enterprise Linux: 8.6 Extended Update Support Long-Life Add-On
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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63888
- https://git.kernel.org/linus/778c2ab142c625a8a8afa570e0f9b7873f445d99
- https://git.kernel.org/stable/c/f7948af0dd03de84079dcd4dc215a69fd6fbb95d
- https://git.kernel.org/stable/c/badf178b76b0690851df00f4ca9cf2eb8eb0f963
- https://git.kernel.org/stable/c/6e22a1cdcc8277af4acc43710577157b77a02c5d
- https://git.kernel.org/stable/c/d3e9b79aa794f7a23e82de4d710e7d2df610e349
- https://git.kernel.org/stable/c/ec9f19d52074a191ed1756ed4a7d39fff1a2085c
- https://git.kernel.org/stable/c/89c81d1228c00fa6dd91de6c1c5aa1ef8a7875e3

- https://git.kernel.org/stable/c/5118ea225fe63b44207ba88047e4866e1ea43812
- https://security-tracker.debian.org/tracker/CVE-2026-63888
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63888
- https://access.redhat.com/security/cve/CVE-2026-63888
- https://ubuntu.com/security/CVE-2026-63888
- https://bdu.fstec.ru/vul/2026-14400

130

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63886
BDU:2026-14399

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

Уязвимый продукт: Linux: от 6.13 до 6.18.34 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63886
- https://git.kernel.org/linus/85db7391310b1304d2dc8ae3b0b12105a9567147
- https://git.kernel.org/stable/c/82454e6f21e56ea9a0a9de7d0ff7e1dfb83e34d6
- https://git.kernel.org/stable/c/edd06675a02376ea8347dba7c29ad982ba5b36ee
- https://git.kernel.org/stable/c/bf154c657828ed05399bca5d98cf1611bb048b12
- https://git.kernel.org/stable/c/4a3a19c98a8207ad08bec554703d90f2c34a8cc6
- https://git.kernel.org/stable/c/c04e85799356120209b351a148ac2db888d5ffd9
- https://security-tracker.debian.org/tracker/CVE-2026-63886

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63886
- https://access.redhat.com/security/cve/CVE-2026-63886
- https://ubuntu.com/security/CVE-2026-63886
- https://bdu.fstec.ru/vul/2026-14399

131

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64150
BDU:2026-14398

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.16 до 6.18.33 включительно
Red Hat Enterprise Linux: 10
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64150
- https://git.kernel.org/linus/a6cb3ff979855f7f0ee9450a947fe8f96c2ba37a
- https://git.kernel.org/stable/c/df19b6af171695a1352314597c9a4311d48d5171
- https://git.kernel.org/stable/c/6fecd39c6401134b58505bc4eb1adc8a0e2fe992
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64150
- https://access.redhat.com/security/cve/CVE-2026-64150
- https://ubuntu.com/security/CVE-2026-64150
- https://bdu.fstec.ru/vul/2026-14398

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64028
BDU:2026-14387

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: 7.0.10
Red Hat Enterprise Linux: 10
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.

132 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64028
- https://git.kernel.org/linus/576ec047d20b368b43c4d5db98c4f2e0f3c101ec
- https://git.kernel.org/stable/c/e3f5d42cdc2f167719564693675f1eead81378ea
- https://git.kernel.org/stable/c/37377b39ff86dacbc533275c1155210d4fd5dc91
- https://git.kernel.org/stable/c/0402a1d3ddec565132867337ed44514a09d84728
- https://git.kernel.org/stable/c/e91687643c440ca3997d67646e6f80b92edc6703
- https://git.kernel.org/stable/c/be4e99038c1603fa6b329d8ee3e364825e17c353
- https://git.kernel.org/stable/c/d6c8b3ebdcdb12b59ad4212acb137cc56cae453d
- https://git.kernel.org/stable/c/915c1254fe0788abddc31095b360e9dc98907a34

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64028
- https://access.redhat.com/security/cve/CVE-2026-64028
- https://bdu.fstec.ru/vul/2026-14387

133

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63922
BDU:2026-14382

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.19 до 5.15.209 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63922
- https://git.kernel.org/linus/f7b52afe3592eae66e160586b45a3f2242972c63
- https://git.kernel.org/stable/c/f8aabed3ff3e986920cf02a2a2785e08e586b234
- https://git.kernel.org/stable/c/1a11eb7431e3d2882f5bd5939c5a9bbc65ccf4d1
- https://git.kernel.org/stable/c/12d957979e4a800167842f1b42be6a606d227ebe
- https://git.kernel.org/stable/c/ff375ed1cba81392346c5bfbf0bb7a13b2946f99
- https://git.kernel.org/stable/c/751db1b802a067b7fff25880f4e9f9152a171538
- https://git.kernel.org/stable/c/9b6dcc0a39fd71752937f0b6b3973e1416085dcf

- https://security-tracker.debian.org/tracker/CVE-2026-63922
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63922
- https://access.redhat.com/security/cve/CVE-2026-63922
- https://ubuntu.com/security/CVE-2026-63922
- https://bdu.fstec.ru/vul/2026-14382

134

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28316
BDU:2026-14381

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28316
- https://bdu.fstec.ru/vul/2026-14381

135

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28314
BDU:2026-14378

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28314
- https://bdu.fstec.ru/vul/2026-14378

136

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28321
BDU:2026-14377

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28321
- https://bdu.fstec.ru/vul/2026-14377

137

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28313
BDU:2026-14376

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28313
- https://bdu.fstec.ru/vul/2026-14376

138

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63924
BDU:2026-14375

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.12 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63924
- https://git.kernel.org/linus/d47548a36639095939f4747d4c43f2271366f565
- https://git.kernel.org/stable/c/b3ac54e5c905f86d22b502eacb5686a282c5659f
- https://git.kernel.org/stable/c/645b99b1a185c91a79bdac4c5de0f91b212d64f0
- https://git.kernel.org/stable/c/9e883eaa878f4337b5873c706efb5a192364ed18
- https://git.kernel.org/stable/c/bddaa4dfc7f36e1ee343a0622f69288af2b9ace9
- https://git.kernel.org/stable/c/72af7beae774e46ed543f3f2f267bf0a141bfcdd
- https://git.kernel.org/stable/c/c512e1c819dfbf6ae95ee7a44b65b9ad98979157

- https://git.kernel.org/stable/c/2b56bbd928c030894c270cd33d60286326919458
- https://security-tracker.debian.org/tracker/CVE-2026-63924
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63924
- https://access.redhat.com/security/cve/CVE-2026-63924
- https://ubuntu.com/security/CVE-2026-63924
- https://bdu.fstec.ru/vul/2026-14375

139

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64104
BDU:2026-14374

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Linux: от 6.13.8 до 6.18.33 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 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: 8.7 AV:L/AC:L/PR:L/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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64104
- https://git.kernel.org/linus/fd948c3f96b18ff9ba7d3e8eae13d196593e1aaf
- https://git.kernel.org/stable/c/bee400ad4f4259c9c0758e4f1960a1eed6f6f9f0
- https://git.kernel.org/stable/c/3d0cd0065deeb054b4b29236432e851806b7cc81
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64104
- https://ubuntu.com/security/CVE-2026-64104
- https://bdu.fstec.ru/vul/2026-14374

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63906
BDU:2026-14373

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.1.2 до 6.1.175 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.

140 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63906
- https://git.kernel.org/linus/e194ce048f5a6c549b3a23a8c568c6470f40f772
- https://git.kernel.org/stable/c/632fd888fe33083927e29ef651ac1aba345edd9e
- https://git.kernel.org/stable/c/b987f380620b38c84f054d5ff5c05861a7c2203b
- https://git.kernel.org/stable/c/27e62532228dc42367bb43ebbcd7bf49d8db2b0d
- https://git.kernel.org/stable/c/69f9f2b30af03d9b6e83f78fb0f734b6066d4678
- https://git.kernel.org/stable/c/d53e4c41331f57b9fd78cbf3e480c6ce20aea07b
- https://security-tracker.debian.org/tracker/CVE-2026-63906
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63906

- https://ubuntu.com/security/CVE-2026-63906
- https://bdu.fstec.ru/vul/2026-14373

141

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64081
BDU:2026-14372

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.15 до 6.18.33 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: 8.4 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64081
- https://git.kernel.org/linus/4a1cc9e96b311d2609a6f963a5e35bd4ae730d97
- https://git.kernel.org/stable/c/3c51d99449dc5a01c08a7fce6071d6721f5aac83
- https://git.kernel.org/stable/c/76eb90e2b03de147e12ab68ea8afd8ea0342df0a
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64081
- https://ubuntu.com/security/CVE-2026-64081
- https://bdu.fstec.ru/vul/2026-14372

142

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28317
BDU:2026-14371

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28317
- https://bdu.fstec.ru/vul/2026-14371

143

Краткое описание: Выполнение произвольного кода в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28312
BDU:2026-14370

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28312
- https://bdu.fstec.ru/vul/2026-14370

144

Краткое описание: Внедрение кода в Linux

Идентификатор уязвимости: CVE-2026-64151
BDU:2026-14369

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Linux: от 6.19 до 7.0.10 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 10

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

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Внедрение 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:L/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64151
- https://git.kernel.org/linus/8ef3f77c440005c7f04229a75976bfc078364247
- https://git.kernel.org/stable/c/00850f41da24423587abd6124a790dd4f12bcef3
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64151
- https://ubuntu.com/security/CVE-2026-64151
- https://bdu.fstec.ru/vul/2026-14369

145

Краткое описание: Выполнение произвольного кода в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28304
BDU:2026-14368

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28304
- https://bdu.fstec.ru/vul/2026-14368

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53380
BDU:2026-14406

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.19 до 7.0.8 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.

146

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53380
- https://git.kernel.org/linus/72773ff1cdfaebc593f53b1719b2c1773ecf8c43
- https://git.kernel.org/stable/c/c746522bd3264132ab2e2382e96e19cdb8a6c1ba
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53380
- https://ubuntu.com/security/CVE-2026-53380
- https://bdu.fstec.ru/vul/2026-14406

147

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53384
BDU:2026-14379

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.9 до 6.1.176 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53384
- https://git.kernel.org/linus/10fc708b4de7f86002d2d735a2dbf3b5b7f65692
- https://git.kernel.org/stable/c/ccdf4510a3873b14e5e348cdb038717996f09fda
- https://git.kernel.org/stable/c/511d2b92f8d20de04acafab676150d26fb5c67f4
- https://git.kernel.org/stable/c/07ffe414a708ae60551401cec5d727ed156b8caf
- https://git.kernel.org/stable/c/3d205fe80f2181f0109150ad1fa06ee5bc046935
- https://git.kernel.org/stable/c/d72650a4f334581b23a1892b888a4cb1be142f76
- https://git.kernel.org/stable/c/778b9dda4b24005a27bcd9c35c110bf8d7f259ca

- https://security-tracker.debian.org/tracker/CVE-2026-53384
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53384
- https://access.redhat.com/security/cve/CVE-2026-53384
- https://ubuntu.com/security/CVE-2026-53384
- https://bdu.fstec.ru/vul/2026-14379

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53389
BDU:2026-14407

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 7.1.2 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.

148

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53389
- https://git.kernel.org/linus/5ba9950bc9078e19b69cca1e56d1553b125c6857
- https://git.kernel.org/stable/c/6ce7ef41743740ce15c2061561b784148b565b3f
- https://git.kernel.org/stable/c/e77fbefd1269b5c123e7c651a1ebdce1b87d19a0
- https://git.kernel.org/stable/c/7ddc29a094d96e9b3aa280433c6dc443df9eabf2
- https://security-tracker.debian.org/tracker/CVE-2026-53389
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53389
- https://ubuntu.com/security/CVE-2026-53389
- https://bdu.fstec.ru/vul/2026-14407

149

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-83941
BDU:2026-14439

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Microsoft Entra ID: -

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: 9.9 AV:N/AC:L/PR:L/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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83941
- https://bdu.fstec.ru/vul/2026-14439

150

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63881
BDU:2026-14409

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.5 до 6.6.142 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63881
- https://git.kernel.org/linus/93f5534b35a05ef8a0109c1eefa800062fee810a
- https://git.kernel.org/stable/c/4e5f808b454167cc58d7084a407a554d8ddc694d
- https://git.kernel.org/stable/c/de70a80992396ee306ee3a2810ad28aa1608ba9b
- https://git.kernel.org/stable/c/5cf4a41aa0d74e4c83f82d2ce233b5189ed4b43c
- https://git.kernel.org/stable/c/4f9eeedc3d3151f8a226fd676c314a813edda5a1
- https://security-tracker.debian.org/tracker/CVE-2026-63881
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63881

- https://access.redhat.com/security/cve/CVE-2026-63881
- https://ubuntu.com/security/CVE-2026-63881
- https://bdu.fstec.ru/vul/2026-14409

151

Краткое описание: Повышение привилегий в Microsoft Power Automate

Идентификатор уязвимости: CVE-2026-65818
BDU:2026-14443

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

Уязвимый продукт: Microsoft Power Platform: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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: 8.5 AV:N/AC:H/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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65818
- https://bdu.fstec.ru/vul/2026-14443

152

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-62916
BDU:2026-14442

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Microsoft Entra ID: -

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: 9.1 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62916
- https://bdu.fstec.ru/vul/2026-14442

153

Краткое описание: Повышение привилегий в Microsoft Copilot Studio

Идентификатор уязвимости: CVE-2026-80098
BDU:2026-14441

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Copilot Studio: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80098
- https://bdu.fstec.ru/vul/2026-14441

154

Краткое описание: Повышение привилегий в Microsoft Azure Active Directory B2C

Идентификатор уязвимости: CVE-2026-83711
BDU:2026-14440

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: Microsoft Azure Active Directory B2C: -

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: 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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83711
- https://bdu.fstec.ru/vul/2026-14440

155

Краткое описание: Выполнение произвольного кода в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28302
BDU:2026-14367

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28302
- https://bdu.fstec.ru/vul/2026-14367

156

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64071
BDU:2026-14438

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.19 до 7.0.10 включительно
Red Hat Enterprise Linux: 10
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64071
- https://git.kernel.org/linus/b35a13036755c5803168a7cb93bc66035c3e65b8
- https://git.kernel.org/stable/c/9525e3a6fbb1d126a22ab2ee86ddea25af581a7c
- https://git.kernel.org/stable/c/7c89f474005d8377525d2991930b7432ee193a52
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64071
- https://access.redhat.com/security/cve/CVE-2026-64071
- https://ubuntu.com/security/CVE-2026-64071
- https://bdu.fstec.ru/vul/2026-14438

157

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63794
BDU:2026-14431

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

Уязвимый продукт: Linux: от 4.16 до 5.10.259 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63794
- https://git.kernel.org/linus/78ee2d50185a037b3d2452a97f3dad69c3f7f389
- https://git.kernel.org/stable/c/f701ae476cb92a3a3d8844bb39bb63b4512684c8
- https://git.kernel.org/stable/c/64f2449841ffc7d203183aa4c748c9c77951ecc5
- https://git.kernel.org/stable/c/9349b50f4b11f135fe73b56cb2c2c872d8bc71d7
- https://git.kernel.org/stable/c/889c2a9c59897ca912bf39df5bb92555a0a13df4
- https://git.kernel.org/stable/c/e1a0fe288dee07b7da25a71e007c1ecd1080315b
- https://git.kernel.org/stable/c/720949ed666f34ff28ffdfe1471a5861d1e41fdf

- https://git.kernel.org/stable/c/2753a097d1fe24c4351c608048612c74108aa89f
- https://security-tracker.debian.org/tracker/CVE-2026-63794
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63794
- https://access.redhat.com/security/cve/CVE-2026-63794
- https://ubuntu.com/security/CVE-2026-63794
- https://bdu.fstec.ru/vul/2026-14431

158

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64191
BDU:2026-14429

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.33 до 5.10.259 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64191
- https://git.kernel.org/linus/6036b5067a8199ba7a2dc7b377d4b9dd276d5f9e
- https://git.kernel.org/stable/c/7e9072dbd5f2f17934751873450d2c22080ead80
- https://git.kernel.org/stable/c/21e87f336ac6303fed54a69b1d0d79a23b25c8d0
- https://git.kernel.org/stable/c/3fd225f3e4cd67ec8ddab1afed9da03c7c43537c
- https://git.kernel.org/stable/c/1c4ffe6b4f04365485ed58d64c9bb86b46fc9037
- https://git.kernel.org/stable/c/4bd8635f28c135a08aac6badcd7d9b5cdb34335f
- https://git.kernel.org/stable/c/5f4d2bd028ebb6e4c09a9d64842546022321d4a7

- https://git.kernel.org/stable/c/0526931b16e5a118d367b7bfce7d797e63f7ac69
- https://security-tracker.debian.org/tracker/CVE-2026-64191
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64191
- https://access.redhat.com/security/cve/CVE-2026-64191
- https://ubuntu.com/security/CVE-2026-64191
- https://bdu.fstec.ru/vul/2026-14429

159

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-64048
BDU:2026-14420

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 5.10 до 6.1.174 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64048
- https://git.kernel.org/linus/277740023def559a4a2ddc3e8e784ee37a0f16a9
- https://git.kernel.org/stable/c/6927cacf2b10d4fa80c1a2d407512ef9397c59c6
- https://git.kernel.org/stable/c/d38ba387244e5c5f7db3e11ea98bc2c7beccb0c0
- https://git.kernel.org/stable/c/53eb7bd09aace72fa17510d80e0caf5ca058c231
- https://git.kernel.org/stable/c/afa9036b8c9963947b487c36e332df6a42c96fcb
- https://git.kernel.org/stable/c/65edb3b0822cfe5041be8fbabebd57e2e5ad9f4e
- https://security-tracker.debian.org/tracker/CVE-2026-64048

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64048
- https://access.redhat.com/security/cve/CVE-2026-64048
- https://ubuntu.com/security/CVE-2026-64048
- https://bdu.fstec.ru/vul/2026-14420

160

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-63983
BDU:2026-14419

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

Уязвимый продукт: Linux: от 6.13 до 7.0.11 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 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63983
- https://git.kernel.org/linus/9552b11e3edabc97cfcd9f29103d5afbce7ae183
- https://git.kernel.org/stable/c/1a298a514ce766c6d0c232991a390fec67af81ad
- https://git.kernel.org/stable/c/cfb2616042767ab31260d4f39190c381bec8b12e
- https://security-tracker.debian.org/tracker/CVE-2026-63983
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63983
- https://access.redhat.com/security/cve/CVE-2026-63983
- https://ubuntu.com/security/CVE-2026-63983

- https://bdu.fstec.ru/vul/2026-14419

161

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-63969
BDU:2026-14418

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

Уязвимый продукт: Linux: от 6.12.2 до 6.12.92 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 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63969
- https://git.kernel.org/linus/9f72412bcf60144f252b0d6205106abf14344abc
- https://git.kernel.org/stable/c/b014a63d2f2c2c767762b548381882dfb1655529
- https://git.kernel.org/stable/c/279853aec9f58d5cd723e6e5617c1c3337b30383
- https://git.kernel.org/stable/c/c65b1f60237daac7c56c2652e064cc566a45dc81
- https://git.kernel.org/stable/c/dc36a04621dcc2447dae428709207810b6c06e14
- https://git.kernel.org/stable/c/5e40de719ee76b8d96e2556ce36dbd3bd07bf37d
- https://security-tracker.debian.org/tracker/CVE-2026-63969

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63969
- https://access.redhat.com/security/cve/CVE-2026-63969
- https://ubuntu.com/security/CVE-2026-63969
- https://bdu.fstec.ru/vul/2026-14418

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-64094
BDU:2026-14417

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 3.5 до 5.10.258 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.

162 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64094
- https://git.kernel.org/linus/f80d3d98d2ff78d9e2fe5d68b1f45948c4f7bd24
- https://git.kernel.org/stable/c/4f6266735a0ba6a568b6d4c9fa51c33a5a7f2d70
- https://git.kernel.org/stable/c/53cb3511f6eda37d3bd923545fdba6013b6d7bb7
- https://git.kernel.org/stable/c/efb62458c94db1fe3a287e7e89c31b0cfb03f938
- https://git.kernel.org/stable/c/2a8c9e86529156c62d9187b9ed9454c31665ad33
- https://git.kernel.org/stable/c/0f3ebd7bb417aabc44853cc7c2a184ebb0e05b45
- https://git.kernel.org/stable/c/6921a7683ae9ad0208d829e71f725a9e25ccff49
- https://git.kernel.org/stable/c/555b8d3f5c313d81d46274fd0976352dafc80124

- https://security-tracker.debian.org/tracker/CVE-2026-64094
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64094
- https://ubuntu.com/security/CVE-2026-64094
- https://bdu.fstec.ru/vul/2026-14417

163

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63869
BDU:2026-14415

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

Уязвимый продукт: Linux: от 6.19 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: 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: 7.6 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63869
- https://git.kernel.org/linus/6c0cf89f36ac0c0fd8687a4ccdce2efb23a9c663
- https://git.kernel.org/stable/c/f6d3dc8e8492bf8435e0b23c99472af7bafd6b44
- https://git.kernel.org/stable/c/9b40c59bab08f2a99abf969cc0bb92fa49de004b
- https://git.kernel.org/stable/c/033ce021a220913ac02416fcb5ac883a9ff8b6c7
- https://security-tracker.debian.org/tracker/CVE-2026-63869
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63869

- https://access.redhat.com/security/cve/CVE-2026-63869
- https://ubuntu.com/security/CVE-2026-63869
- https://bdu.fstec.ru/vul/2026-14415

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63933
BDU:2026-14414

Идентификатор программной ошибки: CWE-369 Деление на ноль

Уязвимый продукт: Linux: от 2.6.35 до 5.10.258 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.

164 **Оценка CVSSv3:** 7.7 AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63933
- https://git.kernel.org/linus/761e8b489e6cf166c574034b70637f8a7eadd0ee
- https://git.kernel.org/stable/c/d2b83995759cfe5d06567bbcb600fe16d4048da3
- https://git.kernel.org/stable/c/19eb8565c4500f9af17ec65eaf952365e2893351
- https://git.kernel.org/stable/c/59f80b945f2ca645064074d8507785c26ea16d2d
- https://git.kernel.org/stable/c/86298fb6829cab983910810959f85d4b4fd0f5c1
- https://git.kernel.org/stable/c/aa8a5e118e97d2cfd0da5ea4f8f0f488efdea4b0
- https://git.kernel.org/stable/c/aaf9d640e9ae1172d0a9c659ecb245a50a10850a
- https://git.kernel.org/stable/c/5a42e39606b9bd6b40ed02bdfd04fe179d6173f4

- https://security-tracker.debian.org/tracker/CVE-2026-63933
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63933
- https://ubuntu.com/security/CVE-2026-63933
- https://bdu.fstec.ru/vul/2026-14414

165

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64050
BDU:2026-14413

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.18 до 6.18.33 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64050
- https://git.kernel.org/linus/c0c70a11365cba7fba25a77463582bcec0f7846e
- https://git.kernel.org/stable/c/ff58e5ef1b46ce614af048d2d04986df05ffab90
- https://git.kernel.org/stable/c/95048a12f48c627bc2ccc4d84f87640630ba2bdb
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64050
- https://ubuntu.com/security/CVE-2026-64050
- https://bdu.fstec.ru/vul/2026-14413

166

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64004
BDU:2026-14412

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 3.4 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64004
- https://git.kernel.org/linus/3589d20a666caf30ad100c960a2de7de390fce88
- https://git.kernel.org/stable/c/884eb247b74d86db97e3a37f0d6fc8e1e83590dd
- https://git.kernel.org/stable/c/45bb8de8c95d8899f4b8f61bd9bceb8132af73cb
- https://git.kernel.org/stable/c/1fc30bd4e55e2dd622d2d366cecd732c1841bbee
- https://git.kernel.org/stable/c/cd691beafea0dd779e69e81ccc26b0ab50efcb5e
- https://git.kernel.org/stable/c/6e792b8dd3002bbc4136745928a9605df1a72b8a
- https://git.kernel.org/stable/c/9817369243380e287ebe5525411557eaa3aa2a79

- https://git.kernel.org/stable/c/69554adc7a6fa04ede3ad7512321d83748e3c920
- https://security-tracker.debian.org/tracker/CVE-2026-64004
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64004
- https://access.redhat.com/security/cve/CVE-2026-64004
- https://ubuntu.com/security/CVE-2026-64004
- https://bdu.fstec.ru/vul/2026-14412

167

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63927
BDU:2026-14411

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63927
- https://git.kernel.org/linus/9ea06a3fbf9f16e0d98c52cb3b99642be15ec281
- https://git.kernel.org/stable/c/d5fc183ed614aeba6779cc992325be560f9a4451
- https://git.kernel.org/stable/c/63b0dafa676aad4d0c3f01a61ad8e2990907660c
- https://git.kernel.org/stable/c/9fe1d84f7e2cf33634e8afb7f4b7f8de182dd913
- https://git.kernel.org/stable/c/0584af4fe40fa5e254a05d69ce658746de641708
- https://git.kernel.org/stable/c/a15eeeceb94cbc04edef395e4d777ff554bdc27d
- https://git.kernel.org/stable/c/84ea928ed584756e59c6ac09736f12d1db95ded0

- https://git.kernel.org/stable/c/6d0b79d1d1118145e48a68192b6d733e39387053
- https://security-tracker.debian.org/tracker/CVE-2026-63927
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63927
- https://access.redhat.com/security/cve/CVE-2026-63927
- https://ubuntu.com/security/CVE-2026-63927
- https://bdu.fstec.ru/vul/2026-14411

168

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63910
BDU:2026-14410

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: Linux: от 7.0 до 7.0.11 включительно
Red Hat Enterprise Linux: 9
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63910
- https://git.kernel.org/linus/ead6680f354f83966c796fc7f9463a3171789616
- https://git.kernel.org/stable/c/b569f86e2f8dbf6f11d31d3de794d22e18098b23
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63910
- https://access.redhat.com/security/cve/CVE-2026-63910
- https://ubuntu.com/security/CVE-2026-63910
- https://bdu.fstec.ru/vul/2026-14410

169

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63855
BDU:2026-14408

Идентификатор программной ошибки: CWE-1012 Сквозные уязвимости

Уязвимый продукт: Linux: от 5.4 до 6.6.140 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63855
- https://git.kernel.org/linus/4f317863a3ab212a027d8c8c3cc3af4e3fb95704
- https://git.kernel.org/stable/c/2c6fb056567efb49f8674108b86088a1cfaa86d0
- https://git.kernel.org/stable/c/8f0ea4524dc71c6c9ec97f2711f46e12f624140f
- https://git.kernel.org/stable/c/602d4c5872b25ddd4d82fb2025efb9a05b187bb3
- https://git.kernel.org/stable/c/5a3c6f76cab164a5d803084908d7050f649ab7f9
- https://ubuntu.com/security/notices/USN-8574-1
- https://security-tracker.debian.org/tracker/CVE-2026-63855

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63855
- https://access.redhat.com/security/cve/CVE-2026-63855
- https://ubuntu.com/security/CVE-2026-63855
- https://bdu.fstec.ru/vul/2026-14408

170

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28310
BDU:2026-14366

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28310
- https://bdu.fstec.ru/vul/2026-14366

171

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64051
BDU:2026-14350

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.4 до 6.6.141 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64051
- https://git.kernel.org/linus/aa16b2bc0f02709919e2435f531406531e5bcc69
- https://git.kernel.org/stable/c/9baafc2fea096279e75480f93fd5942e8336b510
- https://git.kernel.org/stable/c/8dd6edbe26770df147136c3f2ac976c873b82650
- https://git.kernel.org/stable/c/97a8e89cdef36207a8776edc03d6931763a06ad0
- https://git.kernel.org/stable/c/8c795012d0e06b7740e40319b86ff8d2a435098d
- https://security-tracker.debian.org/tracker/CVE-2026-64051
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64051

- https://access.redhat.com/security/cve/CVE-2026-64051
- https://ubuntu.com/security/CVE-2026-64051
- https://bdu.fstec.ru/vul/2026-14350

172

Краткое описание: Выполнение произвольного кода в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28308
BDU:2026-14364

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28308
- https://bdu.fstec.ru/vul/2026-14364

173

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63962
BDU:2026-14334

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 4.19 до 6.12.92 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: 9.1 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63962
- https://git.kernel.org/linus/3389c149c68c3fea61910ad5d34f7bf3bff44e32
- https://git.kernel.org/stable/c/845598b154b9a92e9d279fafafa9405c121ae805
- https://git.kernel.org/stable/c/4505f33dab56c274e82f47f94bf60a8cbf8f4b42
- https://git.kernel.org/stable/c/cbad85b446c06adbc5e5bed565871bb918ce9d32
- https://security-tracker.debian.org/tracker/CVE-2026-63962
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63962
- https://access.redhat.com/security/cve/CVE-2026-63962

- https://ubuntu.com/security/CVE-2026-63962
- https://bdu.fstec.ru/vul/2026-14334

174

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-64106
BDU:2026-14333

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

Уязвимый продукт: Linux: от 4.12 до 6.1.174 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: 9.0 AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64106
- https://git.kernel.org/linus/9ce754ed8e7ab4e3999767ce1505f85c449ccb07
- https://git.kernel.org/stable/c/1716b7fea2ead941a0dfac06c4504a3437cdf00d
- https://git.kernel.org/stable/c/dab9f93251b2c86a033de6098d0c73afddd55d4a
- https://git.kernel.org/stable/c/b94538186a3eae3763b8f96dacd610920a865aa7
- https://git.kernel.org/stable/c/0680f511926589206f81f57f76ce131d7741a316
- https://git.kernel.org/stable/c/8bcd15b690a390241179516af1b6ae49ebfd9d95
- https://security-tracker.debian.org/tracker/CVE-2026-64106

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64106
- https://access.redhat.com/security/cve/CVE-2026-64106
- https://ubuntu.com/security/CVE-2026-64106
- https://bdu.fstec.ru/vul/2026-14333

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63959
BDU:2026-14332

Идентификатор программной ошибки: CWE-130 Некорректная обработка несоответствий параметров длины

Уязвимый продукт: Linux: от 5.10 до 6.6.142 включительно
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.

175

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63959
- https://git.kernel.org/linus/aa2f716327be1818e1cb156da8a2844804aaec2f
- https://git.kernel.org/stable/c/0af00f1459f5dd757f0d392f8caa38039561ac62
- https://git.kernel.org/stable/c/dc17721d42e6d89f63572e63add8306a0e15eb3c
- https://git.kernel.org/stable/c/9b496e3371c04f0a03b7faa5d2442536d00e3998
- https://git.kernel.org/stable/c/c4ab8e2d4432abb646c5c0687f8dab173da901f9
- https://security-tracker.debian.org/tracker/CVE-2026-63959
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63959
- https://ubuntu.com/security/CVE-2026-63959

- https://bdu.fstec.ru/vul/2026-14332

176

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64030
BDU:2026-14331

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.15 до 6.18.33 включительно
Red Hat Enterprise Linux: 10
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: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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64030
- https://git.kernel.org/linus/f718506edd2d9c6a308ded9d13c632bf7b7d5a2c
- https://git.kernel.org/stable/c/2d8379834800c30602f24c71ab7c40f5fe84d200
- https://git.kernel.org/stable/c/863f1f02a3bd70dbd857b8ac4070292fde8cb4e2
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64030
- https://access.redhat.com/security/cve/CVE-2026-64030
- https://ubuntu.com/security/CVE-2026-64030
- https://bdu.fstec.ru/vul/2026-14331

177

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53374
BDU:2026-14329

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Linux: от 4.2 до 6.1.174 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53374
- https://git.kernel.org/linus/e6c2e6c2e1fa066968a16aca1cb66cd1bdde7741
- https://git.kernel.org/stable/c/40df11255d71b02e20e70579f1b12b687e396e26
- https://git.kernel.org/stable/c/91fbb5e635c8fb1b49e15c19da06480089ef719f
- https://git.kernel.org/stable/c/8ae8b9e74bab94aab1d79f1688129bcc61c8b29a
- https://git.kernel.org/stable/c/b17175d0a375b3ed5e81597dac4983fdb46e478d
- https://git.kernel.org/stable/c/791941be5da125d9a1b228582bfdc300c05d05b3
- https://ubuntu.com/security/notices/USN-8574-1

- https://security-tracker.debian.org/tracker/CVE-2026-53374
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53374
- https://access.redhat.com/security/cve/CVE-2026-53374
- https://ubuntu.com/security/CVE-2026-53374
- https://bdu.fstec.ru/vul/2026-14329

178

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53375
BDU:2026-14328

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 4.2 до 6.1.174 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53375
- https://git.kernel.org/linus/de2a02cc28d6d5d37db07d00a9a684c754a5fd74
- https://git.kernel.org/stable/c/2d66d1f5d8c0434e9a5ad21cc6eaf3a5e32141d5
- https://git.kernel.org/stable/c/944db9cfa5373f67eb94621d4c2eee572c05fa3f
- https://git.kernel.org/stable/c/0ee17150763962671f43a62ddf8f6ea1feaff438
- https://git.kernel.org/stable/c/b3d1a0a45c4aec484fa2a5b060b611e3d3064470
- https://git.kernel.org/stable/c/ea2c554e700b86a04534b4c24ece5844e8c5f07e
- https://ubuntu.com/security/notices/USN-8574-1

- https://security-tracker.debian.org/tracker/CVE-2026-53375
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53375
- https://access.redhat.com/security/cve/CVE-2026-53375
- https://ubuntu.com/security/CVE-2026-53375
- https://bdu.fstec.ru/vul/2026-14328

179

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64117
BDU:2026-14327

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.4 до 7.0.10 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: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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64117
- https://git.kernel.org/linus/d71c841be5d9e586ee7f36c0dc8ed4db0d9a1349
- https://git.kernel.org/stable/c/2fb64f94f9afb774f2fa0c7835727d7a67f89f07
- https://security-tracker.debian.org/tracker/CVE-2026-64117
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64117
- https://access.redhat.com/security/cve/CVE-2026-64117
- https://ubuntu.com/security/CVE-2026-64117
- https://bdu.fstec.ru/vul/2026-14327

180

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64124
BDU:2026-14326

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.16 до 6.18.34 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64124
- https://git.kernel.org/linus/4eb82ba543421e9e38cc14e4e82058b78850df50
- https://git.kernel.org/stable/c/134c517dfa63203287b2aad6558017f42435a02e
- https://git.kernel.org/stable/c/d5008e4e4ee6b739256b796702a7d1aae1b5c3b4
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64124
- https://ubuntu.com/security/CVE-2026-64124
- https://bdu.fstec.ru/vul/2026-14326

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64153
BDU:2026-14325

Идентификатор программной ошибки: CWE-253 Некорректная проверка значений, возвращаемых функцией

Уязвимый продукт: Linux: от 6.19 до 7.0.10 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.

181 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64153
- https://git.kernel.org/linus/55e0f0d1c1a4ee1e46da7da4d443eb3044fb3851
- https://git.kernel.org/stable/c/3c2cdb7c07f664b77e2a75b50793b845d5742efa
- https://git.kernel.org/stable/c/3e3c3c95ef4fe17231a9149e27bcfc9dae2dd89f
- https://git.kernel.org/stable/c/7256e54583aee21e23929e7554278c2f5c1a08b1
- https://git.kernel.org/stable/c/3457807aeb88077712f0a7cb65c3ca5120773d75
- https://git.kernel.org/stable/c/f4e37f3df436c2bdd2621c21f9c72c8f149a221d
- https://git.kernel.org/stable/c/3a45af37733446e114bf19b0209fe7d8089bdb8b
- https://ubuntu.com/security/notices/USN-8575-1

- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-64153
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64153
- https://ubuntu.com/security/CVE-2026-64153
- https://bdu.fstec.ru/vul/2026-14325

182

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63863
BDU:2026-14324

Идентификатор программной ошибки: CWE-832 Разблокировка незаблокированного ресурса

Уязвимый продукт: Linux: от 7.0 до 7.0.9 включительно
Red Hat Enterprise Linux: 9
Ubuntu: 26.04 LTS
Debian GNU/Linux: 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: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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63863
- https://git.kernel.org/linus/d287dee565c3c32e1ed76ec1847af46809c29b90
- https://git.kernel.org/stable/c/8efaa47a871662a8c21b819cec60786f7ef17ab4
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63863
- https://access.redhat.com/security/cve/CVE-2026-63863
- https://ubuntu.com/security/CVE-2026-63863
- https://bdu.fstec.ru/vul/2026-14324

183

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63938
BDU:2026-14335

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 6.11 до 6.12.92 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: 9.3 AV:L/AC:L/PR:N/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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63938
- https://git.kernel.org/linus/121d88de56bc5c0ba0ce2f6381af67f948a7e7c1
- https://git.kernel.org/stable/c/5198f70c09a5f6e9e5f5a0a2c6b388f24294b176
- https://git.kernel.org/stable/c/75c8d1d7291268b479794fba5808971dc2f5eaf3
- https://git.kernel.org/stable/c/505a3b94535583e4265360e2621734e355ef263d
- https://security-tracker.debian.org/tracker/CVE-2026-63938
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63938
- https://access.redhat.com/security/cve/CVE-2026-63938

- https://ubuntu.com/security/CVE-2026-63938
- https://bdu.fstec.ru/vul/2026-14335

184

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63865
BDU:2026-14323

Идентификатор программной ошибки: CWE-663 Использование нереентерабельной функции в параллельном контексте

Уязвимый продукт: Linux: от 6.19 до 7.0.9 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 8.8 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63865
- https://git.kernel.org/linus/beaf0e96b1da74549a6cabd040f9667d83b2e97e
- https://git.kernel.org/stable/c/452a927cddcd67478d030e646f41cb904a93156f
- https://git.kernel.org/stable/c/f0fc2a9828171205244a28013f02889f50b71c9f
- https://git.kernel.org/stable/c/26b380a3ca0b605fd8860995ed6a208f276dd316
- https://git.kernel.org/stable/c/0d918263c9bfc86078edb2e2f7302a0c6ce42b7c
- https://git.kernel.org/stable/c/281f2a214565a5cbf8b7355a65738d80bd19b8c5
- https://git.kernel.org/stable/c/989f1b93907de1753a814996222da375f07e579b
- https://ubuntu.com/security/notices/USN-8574-1

- https://ubuntu.com/security/notices/USN-8575-1
- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-63865
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63865
- https://ubuntu.com/security/CVE-2026-63865
- https://bdu.fstec.ru/vul/2026-14323

185

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63921
BDU:2026-14321

Идентификатор программной ошибки: CWE-653 Некорректная изоляция

Уязвимый продукт: Linux: от 3.15 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63921
- https://git.kernel.org/linus/8b484efd5cb4eeef9021a661e198edc5349dacf6
- https://git.kernel.org/stable/c/94ff740a7f9ef5c010784a325dca00cbf228f941
- https://git.kernel.org/stable/c/df42ac708acc3399bbb6dc5ca16e0540adda7bbf
- https://git.kernel.org/stable/c/44d2ff7d2178503b93151140a45dfa2ad49c9906
- https://git.kernel.org/stable/c/1acfb7d9c6fc7e209ed7789392697e97e03edd33
- https://git.kernel.org/stable/c/d2236348414bdd6558385f35aa7fdc9bf5634011
- https://git.kernel.org/stable/c/853f6ea482dfcd3404bbef458ab4d68364eed838

- https://git.kernel.org/stable/c/596f6354c96a891e58c04a09cbfb7b0d1ec00dab
- https://security-tracker.debian.org/tracker/CVE-2026-63921
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63921
- https://access.redhat.com/security/cve/CVE-2026-63921
- https://ubuntu.com/security/CVE-2026-63921
- https://bdu.fstec.ru/vul/2026-14321

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64093
BDU:2026-14320

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 4.8 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 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.

186 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64093
- https://git.kernel.org/linus/d5487249a81ea658717614009c8f46acc5b7101a
- https://git.kernel.org/stable/c/00bf4bb9947b1190a8be8d9b6a1bcbfa3707785c
- https://git.kernel.org/stable/c/74a7663405546283344668fd526d73c290ea43a
- https://git.kernel.org/stable/c/5bc2d50fb66b46f86543d5153a188eb1486d0b6e
- https://git.kernel.org/stable/c/f86b20ec8d17d77bddc02c5c86cfa2389d84ecff
- https://git.kernel.org/stable/c/770bf0a35f0620b526fd4193889d1e77084e4c43
- https://git.kernel.org/stable/c/933880a8bc9b4042223a79255c0b1021cdc36991
- https://security-tracker.debian.org/tracker/CVE-2026-64093

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64093
- https://ubuntu.com/security/CVE-2026-64093
- https://bdu.fstec.ru/vul/2026-14320

187

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64047
BDU:2026-14310

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Linux: от 5.4.14 до 5.10.257 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64047
- https://git.kernel.org/linus/285943c6e7ca309bbea84b253745154241d9788a
- https://git.kernel.org/stable/c/73963a375885d5ccb7def39fd0b4f542e0f343dd
- https://git.kernel.org/stable/c/47110c3a9ac247b688657337f5981efcfcb240dc
- https://git.kernel.org/stable/c/84158c2997159df4a0d70cd9c46774512d32a522
- https://git.kernel.org/stable/c/131ef12057d92b77b636321b7849c69222405a97
- https://git.kernel.org/stable/c/66339b71f105e6f83e0da3b9583d95077534fe1d
- https://git.kernel.org/stable/c/eca989eab4b2599dcb02f72140a7c08f08838520

- https://git.kernel.org/stable/c/2fb0dc7e0099686c4e9d2732745d8a31b18c3628
- https://ubuntu.com/security/notices/USN-8575-1
- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-64047
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64047
- https://access.redhat.com/security/cve/CVE-2026-64047
- https://ubuntu.com/security/CVE-2026-64047
- https://bdu.fstec.ru/vul/2026-14310

188

Краткое описание: Повышение привилегий в MariaDB

Идентификатор уязвимости: BDU:2026-14309

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: MariaDB: 10.6.27

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: 8.8 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: 2026-09-09 / 2026-09-09

Ссылки на источник:

- https://github.com/MariaDB/server/commit/7322a6656a5357b4574b7413493c76ba2fc41f84
- https://hackerone.com/reports/3876430
- https://x.com/kevin_mizu/status/2097055819447550388
- https://bdu.fstec.ru/vul/2026-14309

189

Краткое описание: Повышение привилегий в Windows Update Stack

Идентификатор уязвимости: CVE-2026-81963
BDU:2026-14307

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-09 / 2026-09-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-81963
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-14307

190

Краткое описание: Повышение привилегий в Windows Advanced Local Procedure Call

Идентификатор уязвимости: CVE-2026-85880
BDU:2026-14306

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23397
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23397
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622

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: 2026-09-09 / 2026-09-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-85880
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-14306

191

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64000
BDU:2026-14271

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

Уязвимый продукт: Linux: от 6.13 до 6.18.34 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64000
- https://git.kernel.org/linus/f229426072fc865654a60978bb7fda790a051ff3
- https://git.kernel.org/stable/c/09a37dca090c55ffb1a33f52d8667f1c2367ef48
- https://git.kernel.org/stable/c/a4b64f3e9c7b8259f7dd251a0313420ba7c01852
- https://git.kernel.org/stable/c/71c986c0ba45b7dc574fae27c83e7b6671556f37
- https://git.kernel.org/stable/c/fbd0662f9c9a66e8cc3df3099cca8ed6d3837cc7
- https://git.kernel.org/stable/c/78607a6854a22a2502f68092202e75a39af4865d
- https://security-tracker.debian.org/tracker/CVE-2026-64000

- https://access.redhat.com/security/cve/CVE-2026-64000
- https://ubuntu.com/security/CVE-2026-64000
- https://bdu.fstec.ru/vul/2026-14271

192

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64132
BDU:2026-14270

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.9 до 6.12.91 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64132
- https://git.kernel.org/linus/e46e6bc97fb1f339730ff1ba74267fbf48e7a422
- https://git.kernel.org/stable/c/769723124b7c3b2bfea4cf68ad292698b87c8d01
- https://git.kernel.org/stable/c/24de676da63c1122d2c13b0d546238b66d1b4e62
- https://git.kernel.org/stable/c/5af905aa8e91ff8d94572a1e089558f21dcf24ed
- https://security-tracker.debian.org/tracker/CVE-2026-64132
- https://access.redhat.com/security/cve/CVE-2026-64132
- https://ubuntu.com/security/CVE-2026-64132

- https://bdu.fstec.ru/vul/2026-14270

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64091
BDU:2026-14269

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: Linux: от 4.17 до 5.10.258 включительно
Ubuntu: 26.04 LTS
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.

193 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64091
- https://git.kernel.org/linus/94d27005016be15ffc638b2ecbc4d58805ad7b48
- https://git.kernel.org/stable/c/e4236bf3ec8d6bb15d0d8d825dcf9933a7d6666b
- https://git.kernel.org/stable/c/724a8eb4155669797c96b70d70e354284ae3b5a8
- https://git.kernel.org/stable/c/211ea59988e1cba43cb0367ad65d379b56f9c3bd
- https://git.kernel.org/stable/c/65a1e67339aa8c95ac544b796946af388930ee23
- https://git.kernel.org/stable/c/b4d4efd4e351593c81e9293d4b4408d244fa5ee7
- https://git.kernel.org/stable/c/4cc85aec8d3c9ab4dc716dc9f1ed36fca16b227f
- https://git.kernel.org/stable/c/9a9c859457bc440a55773e01ff18b1bb5bab6836

- https://security-tracker.debian.org/tracker/CVE-2026-64091
- https://ubuntu.com/security/CVE-2026-64091
- https://bdu.fstec.ru/vul/2026-14269

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63795
BDU:2026-14268

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.0 до 6.1.176 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.

194 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63795
- https://git.kernel.org/linus/1a3860d46e3eb47dbd60339783cdad7904486b9f
- https://git.kernel.org/stable/c/99c379ca1e221c3d75c7c804ebbf4e5ee37a3070
- https://git.kernel.org/stable/c/b84f46179c806450b89821221ea5bd9a1698aba8
- https://git.kernel.org/stable/c/a61bdcba4f64c2f90d01461913f429ab151f1ca6
- https://git.kernel.org/stable/c/6dbe9443d9f5f7fb6d319a7b77108853ae6c6bea
- https://git.kernel.org/stable/c/a7656d368265d085ac9bb85ab31b0cdb72ad8c38
- https://security-tracker.debian.org/tracker/CVE-2026-63795
- https://ubuntu.com/security/CVE-2026-63795

- https://bdu.fstec.ru/vul/2026-14268

195

Краткое описание: Отказ в обслуживании в PyPDF

Идентификатор уязвимости: CVE-2026-84309
BDU:2026-14262

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

Уязвимый продукт: PyPDF: до 6.16.0

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: 2026-09-09 / 2026-09-09

Ссылки на источник:

- https://github.com/py-pdf/pypdf/pull/3964
- https://github.com/py-pdf/pypdf/releases/tag/6.16.0
- https://github.com/py-pdf/pypdf/security/advisories/GHSA-jp53-mhqp-8xcg
- https://dailycve.com/pypdf-infinite-loop-cwe-835-cve-2026-84309-moderate-dc-sep2026-2075/
- https://bdu.fstec.ru/vul/2026-14262

196

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63885
BDU:2026-14322

Идентификатор программной ошибки: CWE-366 Состояние гонки в потоке

Уязвимый продукт: Linux: от 7.0.9 до 7.0.11 включительно
Red Hat Enterprise Linux: 10
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: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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63885
- https://git.kernel.org/linus/7164d78559b0ff29931a366a840a9e5dd53d4b7c
- https://git.kernel.org/stable/c/0dfa42cfe4dbe114533480503934f43e33c1e83d
- https://git.kernel.org/stable/c/cde2c9257cbe8463b9dcf7b1075177b72b5fd938
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63885
- https://access.redhat.com/security/cve/CVE-2026-63885
- https://bdu.fstec.ru/vul/2026-14322

197

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28309
BDU:2026-14365

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28309
- https://bdu.fstec.ru/vul/2026-14365

198

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64090
BDU:2026-14336

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

Уязвимый продукт: Linux: от 3.13 до 5.10.258 включительно
Ubuntu: 26.04 LTS
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.

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64090
- https://git.kernel.org/linus/fa1bd704940b5bcbc32c0b28db9167405c8ee5e0
- https://git.kernel.org/stable/c/1f467d9a095211d3f77e8ff1bee90e73ffe01c64
- https://git.kernel.org/stable/c/9a02c8fc963ddeecb5d8788be0740c1869fc54b7
- https://git.kernel.org/stable/c/ea4f757641430bcc8322772e161453c4db5ecb64
- https://git.kernel.org/stable/c/99f17d1cdb371cbd037975239b321f346d38f6d2
- https://git.kernel.org/stable/c/cfb30645280a2131e46cbd1b9a38cfd3ff893f12
- https://git.kernel.org/stable/c/b93ca6012712ecab2b551e120d7c95038d6a89e5
- https://git.kernel.org/stable/c/ab26e346322648f5c39de017d9723c9256284fce

- https://security-tracker.debian.org/tracker/CVE-2026-64090
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64090
- https://ubuntu.com/security/CVE-2026-64090
- https://bdu.fstec.ru/vul/2026-14336

199

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63870
BDU:2026-14338

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Linux: от 4.0 до 5.10.258 включительно
Red Hat Enterprise Linux: 9
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63870
- https://git.kernel.org/linus/3a5f3f7aff18bcc36a57839cf50cf0cc8de707f3
- https://git.kernel.org/stable/c/af07fffbd53ddc3ec3c2a4ca914f27899fa89bca
- https://git.kernel.org/stable/c/3150e6d3223dfc356308125cabf9c34169842d2a
- https://git.kernel.org/stable/c/8da95cb6ad7d656c871e776a9c7b77e894d6d89c
- https://git.kernel.org/stable/c/1a827b95e62b4cbe851ae7cc9c961cdfa769cca4
- https://git.kernel.org/stable/c/c1819c8defa235c7beda859bc185b1c429a55ecd
- https://git.kernel.org/stable/c/285b0842f2e01c3edf805f1fd64da11d9b7f6b4c

- https://git.kernel.org/stable/c/87172cc8dc49aaf54407a31edffb0232f8cb93ab
- https://security-tracker.debian.org/tracker/CVE-2026-63870
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63870
- https://access.redhat.com/security/cve/CVE-2026-63870
- https://ubuntu.com/security/CVE-2026-63870
- https://bdu.fstec.ru/vul/2026-14338

200

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28307
BDU:2026-14363

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28307
- https://bdu.fstec.ru/vul/2026-14363

201

Краткое описание: Повышение привилегий в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28306
BDU:2026-14362

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28306
- https://bdu.fstec.ru/vul/2026-14362

202

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63864
BDU:2026-14361

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: Linux: от 6.19 до 7.0.9 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 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: 8.4 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63864
- https://git.kernel.org/linus/6bd96e40f31dde8f8cd79772b4df0f171cf8a915
- https://git.kernel.org/stable/c/945816e63c8677cf4bfde963a0774432ce8afc85
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63864
- https://access.redhat.com/security/cve/CVE-2026-63864
- https://ubuntu.com/security/CVE-2026-63864
- https://bdu.fstec.ru/vul/2026-14361

203

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64045
BDU:2026-14360

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.16 до 6.18.33 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: 8.4 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64045
- https://git.kernel.org/linus/775d8d7ad02aa345e1588424a6a8b9ae49fb9012
- https://git.kernel.org/stable/c/e5460eb7238c19d651a9b22b2378b587033a4095
- https://git.kernel.org/stable/c/d3ef441907fca7c340979e577a3db3bb634bf166
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64045
- https://ubuntu.com/security/CVE-2026-64045
- https://bdu.fstec.ru/vul/2026-14360

204

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63926
BDU:2026-14359

Идентификатор программной ошибки: CWE-823 Использование для указателя смещения за пределами назначенного диапазона

Уязвимый продукт: Linux: от 4.20 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: 8.4 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63926
- https://git.kernel.org/linus/f72eed9b84fb771019a955908132410a9ba9ea3f
- https://git.kernel.org/stable/c/f14609d8146707452e0822f3c8154674ce677251
- https://git.kernel.org/stable/c/d81b323af2dcee47573907ccb89c0df9b45cb2e2
- https://git.kernel.org/stable/c/aeb95146848d12206e1b2cfacd4f40e21ce81d94
- https://git.kernel.org/stable/c/96b72672ce849a1402730238e64d9b20bf06a96d
- https://git.kernel.org/stable/c/3075c21d2d76c0067f4a382765b43d6cc10470f1
- https://git.kernel.org/stable/c/5e19028667963fb371ebb00cecc2a473ef92056b

- https://git.kernel.org/stable/c/63f64a510c7917658ddf4d073ece73914ee25346
- https://security-tracker.debian.org/tracker/CVE-2026-63926
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63926
- https://access.redhat.com/security/cve/CVE-2026-63926
- https://ubuntu.com/security/CVE-2026-63926
- https://bdu.fstec.ru/vul/2026-14359

205

Краткое описание: Выполнение произвольного кода в SolarWinds Serv-U

Идентификатор уязвимости: CVE-2026-28305
BDU:2026-14358

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SolarWinds Serv-U: до 15.5.4 HF1 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm
- https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28305
- https://bdu.fstec.ru/vul/2026-14358

206

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64135
BDU:2026-14357

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: Linux: от 5.10 до 5.10.257 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: 8.2 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64135
- https://git.kernel.org/linus/eee213daa1e1b402eb631bcd1b8c5aa340a6b081
- https://git.kernel.org/stable/c/33251abb9c9dd62943be76f0427c5527ee39188f
- https://git.kernel.org/stable/c/ba09f4baa5bd96c5d26c942defa546a72dbbe5bf
- https://git.kernel.org/stable/c/6ed16a40b162e9d87d9ac8bed4d7f0e3e807700e
- https://git.kernel.org/stable/c/0dbf64c502443c08c2e28a77ecbfcc5479d93228
- https://git.kernel.org/stable/c/2b7a698d5093b548c464828d984f05ced5f3fd2a
- https://git.kernel.org/stable/c/ca560f7566df7e2826c2999e959e6b94eb938f76
- https://git.kernel.org/stable/c/7f705e581ef3e6bb308a121a89adf5237d968204

- https://ubuntu.com/security/notices/USN-8575-1
- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-64135
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64135
- https://ubuntu.com/security/CVE-2026-64135
- https://bdu.fstec.ru/vul/2026-14357

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64169
BDU:2026-14356

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Linux: от 6.12 до 6.12.91 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.

207

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64169
- https://git.kernel.org/linus/5e121a81667a83e9a01d62b429e340f5a4a84abc
- https://git.kernel.org/stable/c/b6c0dabea07e25bd7db19a77ebfd0d02b9e2671a
- https://git.kernel.org/stable/c/8e027db9fa310b1d5e7ad928510be800c4f004d9
- https://git.kernel.org/stable/c/0e2189ab095e3657f37b8295f3f2bbcde0f27529
- https://security-tracker.debian.org/tracker/CVE-2026-64169
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64169
- https://ubuntu.com/security/CVE-2026-64169
- https://bdu.fstec.ru/vul/2026-14356

208

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-63913
BDU:2026-14355

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Linux: от 2.6.15 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: Злоупотребление функционалом.

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63913
- https://git.kernel.org/linus/bed6e04be8e6b9133d8b16d5a42d0e0ce674fa9a
- https://git.kernel.org/stable/c/2006979a15af5404bf932a325357683c0bac1656
- https://git.kernel.org/stable/c/6476c17d536dbd321c073242e762ddb2713a1238
- https://git.kernel.org/stable/c/f5547bebc416d56f56fb5b86dc20aabfa42165a0
- https://git.kernel.org/stable/c/2bb6d82b586ea5a4cb73bbdd6b7432e96096bc77
- https://git.kernel.org/stable/c/f206def4e86d810f927ba1d8e322ea72b29bce58
- https://git.kernel.org/stable/c/b98ab51c45c5608a1c19ce7fd17a3032469bb83f

- https://git.kernel.org/stable/c/d67c6adee8d1b65330d0174c4c367faba14e80a8
- https://security-tracker.debian.org/tracker/CVE-2026-63913
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63913
- https://access.redhat.com/security/cve/CVE-2026-63913
- https://ubuntu.com/security/CVE-2026-63913
- https://bdu.fstec.ru/vul/2026-14355

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-63893
BDU:2026-14354

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.13 до 6.18.34 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.

209

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63893
- https://git.kernel.org/linus/01deda0152066c6c955f0619114ea6afa070aaec
- https://git.kernel.org/stable/c/6a63623621639acbb39bc2d9fb09559681716695
- https://git.kernel.org/stable/c/e8a0b0a93a6ef958e70b1dd4930beb6dc0026b36
- https://git.kernel.org/stable/c/9fee50c4e1e42f6d3cbe30df584f9f648f626071
- https://git.kernel.org/stable/c/8d4a758b407ab3de3be86d1ceadfa35d717d30c7
- https://git.kernel.org/stable/c/5c06a3043ad944f087bb2ae0aae28d820bb9f460
- https://git.kernel.org/stable/c/31b98e503ecca8077e5247253dd5425ab84bc96d
- https://git.kernel.org/stable/c/a47784aee77f33f786dc5d7375db821bdae68792

- https://security-tracker.debian.org/tracker/CVE-2026-63893
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63893
- https://ubuntu.com/security/CVE-2026-63893
- https://bdu.fstec.ru/vul/2026-14354

210

Краткое описание: Выполнение произвольного кода в MongoDB Server

Идентификатор уязвимости: CVE-2026-8201
BDU:2026-14353

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: MongoDB Server: от 8.3 до 8.3.2

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: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://jira.mongodb.org/browse/SERVER-122032
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-40530
- https://bdu.fstec.ru/vul/2026-14353

211

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63971
BDU:2026-14337

Идентификатор программной ошибки: CWE-165 Некорректная нейтрализация множественных специальных элементов в середине

Уязвимый продукт: Linux: от 4.16 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: 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63971
- https://git.kernel.org/linus/f14fe6395a8b3d961a61e138ad7b36ba3626dd4e
- https://git.kernel.org/stable/c/0e0d5bc76fd4267a71334fcc8f1a5fbcf997845d
- https://git.kernel.org/stable/c/bcfeac79af740735ace44008b4a11b8e5add20f5
- https://git.kernel.org/stable/c/8e9b56051d24540cfbf39194618708c4a7633549
- https://git.kernel.org/stable/c/634a9af8a26a84d8b0d7b3b643204b344b42d9fb
- https://git.kernel.org/stable/c/7d2038d4b80166f7bead8d07eba3b97405816c21
- https://git.kernel.org/stable/c/68667ee4c7dadf7f63167234e2a1af09b3f7874e

- https://git.kernel.org/stable/c/6140cfa721451fa6e18e134e709703c2bf34d0fb
- https://security-tracker.debian.org/tracker/CVE-2026-63971
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63971
- https://access.redhat.com/security/cve/CVE-2026-63971
- https://ubuntu.com/security/CVE-2026-63971
- https://bdu.fstec.ru/vul/2026-14337

212

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53401
BDU:2026-14349

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.36 до 7.1.2 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53401
- https://git.kernel.org/linus/7958e67375aa111522086286bba13cfc0816ce8d
- https://git.kernel.org/stable/c/6eb6ebcc8590007ad59ddccc8b5f9201655b33f8
- https://security-tracker.debian.org/tracker/CVE-2026-53401
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53401
- https://ubuntu.com/security/CVE-2026-53401
- https://bdu.fstec.ru/vul/2026-14349

213

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63918
BDU:2026-14348

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

Уязвимый продукт: Linux: от 6.12 до 6.12.92 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63918
- https://git.kernel.org/linus/05f95729ca844704d15e49ce14868af4b403b32b
- https://git.kernel.org/stable/c/ee80455feffb9cb62b5b58715cabeff495e666b2
- https://git.kernel.org/stable/c/947013fd7c8c35dd5856557b215840098a3f67f8
- https://git.kernel.org/stable/c/782d60a6596aee9b29c2eecfa70033899278bf65
- https://security-tracker.debian.org/tracker/CVE-2026-63918
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63918
- https://access.redhat.com/security/cve/CVE-2026-63918

- https://ubuntu.com/security/CVE-2026-63918
- https://bdu.fstec.ru/vul/2026-14348

214

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64002
BDU:2026-14347

Идентификатор программной ошибки: CWE-459 Неполная очистка

Уязвимый продукт: Linux: от 3.16 до 5.10.258 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64002
- https://git.kernel.org/linus/87a1e0fe7776da7ab411be332b4be58ac8840d10
- https://git.kernel.org/stable/c/ecf45080a4d3f4526cacb8b14060fe3b49a6913b
- https://git.kernel.org/stable/c/a0ffc6081a8b27082dd5eae5aa1e3f59bbecf06c
- https://git.kernel.org/stable/c/5b23a2ff379e70b6b9ff744a972b63e1f8f4d996
- https://git.kernel.org/stable/c/8e59d4d0dcde2dfb07a7ef855c849a2a0560aa57
- https://git.kernel.org/stable/c/6512c57c4638ddec113bf42439361ba85a12048d
- https://git.kernel.org/stable/c/a7f4eefb6e1458431eef9fa20fb363320d185f76

- https://git.kernel.org/stable/c/155f90be5ee8be5b110ebc0b7da33c54c83b0208
- https://security-tracker.debian.org/tracker/CVE-2026-64002
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64002
- https://access.redhat.com/security/cve/CVE-2026-64002
- https://ubuntu.com/security/CVE-2026-64002
- https://bdu.fstec.ru/vul/2026-14347

215

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64008
BDU:2026-14346

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.18 до 6.18.34 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64008
- https://git.kernel.org/linus/f706e6a4ce75585af979aec3dcbdce68bc76306b
- https://git.kernel.org/stable/c/18abd88d19ea195e2e1547fca0970c2f91d77a42
- https://git.kernel.org/stable/c/451f1ccbbdb7b65021646704b15902655f8d228a
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64008
- https://ubuntu.com/security/CVE-2026-64008
- https://bdu.fstec.ru/vul/2026-14346

216

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64053
BDU:2026-14345

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.11 до 6.12.91 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64053
- https://git.kernel.org/linus/637ad3a56a3b889527d1dacea6fea2a8bd648140
- https://git.kernel.org/stable/c/d18160c9525c63c203656fefd847e94b538cd4a4
- https://git.kernel.org/stable/c/0d48654af4d1390c888389206cc13b51b82c30e6
- https://git.kernel.org/stable/c/066be1439593a381b1a29663becfcfe0c92363e7
- https://security-tracker.debian.org/tracker/CVE-2026-64053
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64053
- https://access.redhat.com/security/cve/CVE-2026-64053

- https://ubuntu.com/security/CVE-2026-64053
- https://bdu.fstec.ru/vul/2026-14345

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64084
BDU:2026-14344

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.10 до 5.10.257 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.

217 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-64084
- https://git.kernel.org/linus/d7834d92251baade796812876e95555e2066fa9f
- https://git.kernel.org/stable/c/d0593e15fdeb56048a72c5c6e720f702759d0ccd
- https://git.kernel.org/stable/c/17cee2f59029039416e8f6303050038eb59ba149
- https://git.kernel.org/stable/c/299efd14c2eda7e5fd40025e54addd4151a01081
- https://git.kernel.org/stable/c/4d1da9a6be5a8156c532d571c2ed237169f99244
- https://git.kernel.org/stable/c/b96c7f0bc0713dc6403912f6527d4ff9168d6fe6
- https://git.kernel.org/stable/c/fa7ca363069a70b0d1aa51e8892e3095fe2ac1ec
- https://git.kernel.org/stable/c/2aef8f08c479f4cbc83e1e6b19d1c94d4dd24f17

- https://ubuntu.com/security/notices/USN-8575-1
- https://ubuntu.com/security/notices/USN-8576-1
- https://security-tracker.debian.org/tracker/CVE-2026-64084
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-64084
- https://ubuntu.com/security/CVE-2026-64084
- https://bdu.fstec.ru/vul/2026-14344

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-53386
BDU:2026-14343

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.9 до 6.12.94 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.

218 **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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-53386
- https://git.kernel.org/linus/95e8a48d7a85d4226934020e57815a3316d3a14b
- https://git.kernel.org/stable/c/d5793975fc3b1780ba576812158ef22e3104e60e
- https://git.kernel.org/stable/c/d08d82d83ed45fd8c001a9df66ad7ebb86c9d6c6
- https://git.kernel.org/stable/c/abe0854e356b1bb814393ca884cb42b3eb12ce10
- https://git.kernel.org/stable/c/abd776ded3e256889610595290f6ca46cb6e91ab
- https://security-tracker.debian.org/tracker/CVE-2026-53386
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-53386
- https://ubuntu.com/security/CVE-2026-53386

- https://bdu.fstec.ru/vul/2026-14343

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63799
BDU:2026-14342

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19 до 7.1.2 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.

219

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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63799
- https://git.kernel.org/linus/de3ab9bd3133899efb92e4cd05ba4203e58fc0a3
- https://git.kernel.org/stable/c/8d32856fb72ba976d9c87ba405fd17e80419934c
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63799
- https://ubuntu.com/security/CVE-2026-63799
- https://bdu.fstec.ru/vul/2026-14342

220

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63809
BDU:2026-14341

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

Уязвимый продукт: Linux: от 5.11.3 до 5.15.210 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63809
- https://git.kernel.org/linus/4c21b5927d4364bfe7365f2700da5fea0ed0d004
- https://git.kernel.org/stable/c/d0a81ed5ff5d0f9c3f63a4f9e5a4642c363ecd3e
- https://git.kernel.org/stable/c/77355ef7a9f6b0d2bdf65be3b37f2c1f365e20d2
- https://git.kernel.org/stable/c/e1d1e203a6000804c5d3b8a4aa4e52303c0c7ab2
- https://git.kernel.org/stable/c/81fc9a13acae99966232f0e055eb2e445263b89a
- https://git.kernel.org/stable/c/838fe9c28121777c59a9406710a68fcf77bb8017
- https://git.kernel.org/stable/c/65bd0c0afb0e1bf3287458e342429b069624f7d4

- https://git.kernel.org/stable/c/70df4de46577fab5e25418f014583155a147c902
- https://security-tracker.debian.org/tracker/CVE-2026-63809
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63809
- https://access.redhat.com/security/cve/CVE-2026-63809
- https://ubuntu.com/security/CVE-2026-63809
- https://bdu.fstec.ru/vul/2026-14341

221

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63824
BDU:2026-14340

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 4.20 до 5.10.259 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63824
- https://git.kernel.org/linus/cb481e59ea6cae3b7796ac1d7a22b6b24c3f3c0b
- https://git.kernel.org/stable/c/622ec2dcd59f21623f2a7ab773c80ceb7d555e3a
- https://git.kernel.org/stable/c/b1e247338bc71826a2d2def3e0874c34749df69a
- https://git.kernel.org/stable/c/0f3058d7d26f81df9b68a18ddbe164bdc3c5eff3
- https://git.kernel.org/stable/c/5966e4e2ba213ab7ad559166152eb4f1f170dd2c
- https://git.kernel.org/stable/c/5165f1cc727f1322456735df212d8e26ec237a8d
- https://git.kernel.org/stable/c/b11c1fa32667692a2c0566e10163758e786e430c

- https://git.kernel.org/stable/c/670fc6a311ed321522b7fff92cf0fc376b4f6e78
- https://security-tracker.debian.org/tracker/CVE-2026-63824
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63824
- https://access.redhat.com/security/cve/CVE-2026-63824
- https://ubuntu.com/security/CVE-2026-63824
- https://bdu.fstec.ru/vul/2026-14340

222

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-63854
BDU:2026-14339

Идентификатор программной ошибки: CWE-1012 Сквозные уязвимости

Уязвимый продукт: Linux: от 5.9 до 6.6.140 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: 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: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63854
- https://git.kernel.org/linus/f1e5a6660d7cbf006079126d9babbf0ccf538c6b
- https://git.kernel.org/stable/c/e74fc9c72c1ba78d0de0b849f5929c3b39a8e20c
- https://git.kernel.org/stable/c/26c4f38529ac78930c9c4713e16ebc5b689bb0a3
- https://git.kernel.org/stable/c/2d6525e7b2504f5bbfe9417cddc1e8da858791dd
- https://git.kernel.org/stable/c/b076e45e6f757a2829e80d0144c1b5f201bee5af
- https://ubuntu.com/security/notices/USN-8574-1
- https://security-tracker.debian.org/tracker/CVE-2026-63854

- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63854
- https://access.redhat.com/security/cve/CVE-2026-63854
- https://ubuntu.com/security/CVE-2026-63854
- https://bdu.fstec.ru/vul/2026-14339

223

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-63925
BDU:2026-14351

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: Linux: от 5.7 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: Нарушение аутентификации.

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:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-08 / 2026-09-08

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-63925
- https://git.kernel.org/linus/e68842b3356471ba56c882209f324613dac47f64
- https://git.kernel.org/stable/c/dd7306779c6ce1238f4cdc34f3c1f2246b854457
- https://git.kernel.org/stable/c/d15130461df388136b62a7b0ce9f66e7e2fa9ff1
- https://git.kernel.org/stable/c/23c0e230eab397d7f68be2538790ac41d3bb91fd
- https://git.kernel.org/stable/c/679e13a65e68a67c8b3c0467c02ee89157ec6f0f
- https://git.kernel.org/stable/c/79495a1b0944fe31ffd54b54b00211b493590d62
- https://git.kernel.org/stable/c/6d00f5c7e5ff7ec4795b7f5f8ed88bd346641652

- https://git.kernel.org/stable/c/d55acbe577db892b60547b6ef1c020b359331a6d
- https://security-tracker.debian.org/tracker/CVE-2026-63925
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-63925
- https://access.redhat.com/security/cve/CVE-2026-63925
- https://ubuntu.com/security/CVE-2026-63925
- https://bdu.fstec.ru/vul/2026-14351

224

Краткое описание: Выполнение произвольного кода в MikroTik RouterOS

Идентификатор уязвимости: CVE-2026-67281

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

Уязвимый продукт: MikroTik RouterOS: от 7.24 до 7.24.2
MikroTik RouterOS: от 7.20 до 7.23.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Не определено

Оценка CVSSv3: Не определено

Оценка CVSSv4: 0.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801
- https://forum.mikrotik.com/t/7-24-2-stable-is-released/272800
- https://mikrotik.com/supportsec/september-2026-vulnerability/

225

Краткое описание: Отказ в обслуживании в MikroTik RouterOS

Идентификатор уязвимости: CVE-2026-67277
BDU:2026-14157

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: MikroTik RouterOS: от 6.0.0 до 6.49.21
MikroTik RouterOS: от 7.0.0 до 7.23.4
MikroTik RouterOS: от 7.24 до 7.24.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://forum.mikrotik.com/t/6-49-21-long-term-is-released/272802
- https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801
- https://forum.mikrotik.com/t/7-24-2-stable-is-released/272800

226

Краткое описание: Повышение привилегий в MikroTik RouterOS

Идентификатор уязвимости: CVE-2026-86060
BDU:2026-14154

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: MikroTik RouterOS: от 6.0.0 до 6.49.21
MikroTik RouterOS: от 7.0.0 до 7.23.4
MikroTik RouterOS: от 7.24 до 7.24.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://forum.mikrotik.com/t/6-49-21-long-term-is-released/272802
- https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801
- https://forum.mikrotik.com/t/7-24-2-stable-is-released/272800

227

Краткое описание: Запись локальных файлов в MikroTik RouterOS

Идентификатор уязвимости: CVE-2026-67276
BDU:2026-14153

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: MikroTik RouterOS: от 6.0.0 до 6.49.21
MikroTik RouterOS: от 7.0.0 до 7.23.4
MikroTik RouterOS: от 7.24 до 7.24.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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: 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: 2026-09-07 / 2026-09-07

Ссылки на источник:

- https://forum.mikrotik.com/t/6-49-21-long-term-is-released/272802
- https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801
- https://forum.mikrotik.com/t/7-24-2-stable-is-released/272800

228

Краткое описание: Выполнение произвольного кода в Cisco IOS XR Software

Идентификатор уязвимости: CVE-2026-20277

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Cisco IOS XR Software: 6.5.29, 7.0.1, 6.5.26, 6.5.25, 6.5.28, 6.5.90, 7.1.1, 7.0.90, 6.7.1, 7.0.2, 7.1.15, 7.2.1, 7.1.2, 6.7.2, 7.0.11, 7.0.12, 7.0.14, 7.1.25, 7.2.12, 7.3.1, 7.1.3, 6.7.3, 7.4.1, 7.2.2, 6.7.4, 6.5.31, 7.3.15, 7.3.16, 6.8.1, 7.4.15, 6.5.32, 7.3.2, 7.5.1, 7.4.16, 7.3.27, 7.6.1, 7.5.2, 7.8.1, 7.6.15, 7.5.12, 7.8.12, 7.3.3, 6.8.2, 7.3.4, 7.4.2, 6.7.35, 6.9.1, 7.6.2, 7.5.3, 7.7.2, 6.9.2, 7.9.1, 7.10.1, 7.8.2, 7.5.4, 6.5.33, 7.8.22, 7.7.21, 7.9.2, 7.3.5, 7.5.5, 7.11.1, 7.9.21, 7.10.2, 24.1.1, 7.6.3, 7.3.6, 7.5.52, 7.11.2, 24.2.1, 24.1.2, 24.2.11, 24.3.1, 24.4.1, 24.2.2, 7.8.23, 7.11.21, 24.2.20, 24.3.2, 24.4.10, 6.5.35, 25.1.1, 24.4.2, 24.3.20, 24.4.15, 25.2.1, 6.5.351, 25.1.2, 24.3.30, 25.3.1, 6.5.352, 24.4.30, 24.2.21, 25.4.1, 25.2.2, 25.2.15, 7.2.0, 7.0.0, 25.2.30, 6.5.353, 26.1.1, 25.1.30, 25.3.15, 26.2.100, 25.4.2, 26.2.1, 25.4.30, 26.1.2, 25.4.201, 26.2.101

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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: 2026-09-02 / 2026-09-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/cve-2026-20277
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM

Краткое описание: Выполнение произвольного кода в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2026-20212

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Cisco NX-OS Software: 10.3(1), 10.3(2), 10.3(3), 10.4(1), 10.3(99w), 10.3(3w), 10.3(99x), 10.3(3o), 10.3(4), 10.3(3p), 10.3(4a), 10.4(2), 10.3(3q), 10.3(5), 10.4(3), 10.3(3x), 10.3(4g), 10.5(1), 10.3(3r), 10.3(6), 10.4(4), 10.3(4h), 10.5(2), 10.3(7), 10.4(5), 10.5(3), 10.4(4g), 10.5(4), 10.6(1), 10.5(3t), 10.3(8), 10.4(6), 10.5(3s), 10.5(3e), 10.5(3o), 10.6(1s), 10.6(2), 10.5(3p), 10.3(9), 10.6(2s), 10.6(3), 10.4(7), 10.5(5), 10.6(2n), 10.6(3s)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

229 **Рекомендации по устранению:** Данная уязвимость устраняется официальным 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 / 2026-09-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/cve-2026-20212
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr

230

Краткое описание: Выполнение произвольного кода в FortiManager

Идентификатор уязвимости: CVE-2026-70468

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: FortiManager: 7.6.1, с 7.4.3 по 7.4.5, с 7.2.5 по 7.2.9
FortiManager Cloud: 7.6.1, с 7.4.3 по 7.4.5, с 7.2.5 по 7.2.9

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса 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.

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: 2026-08-12 / 2026-09-08

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/cve-2026-70468
- https://fortiguard.fortinet.com/psirt/FG-IR-26-160