НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-02-23.1 | 23 февраля 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-2649	Microsoft Edge	Сетевой	ACE	2026-02-21	✓
2	Высокая	CVE-2026-2648	Microsoft Edge	Сетевой	ACE	2026-02-21	✓
3	Высокая	CVE-2026-2650	Microsoft Edge	Сетевой	ACE	2026-02-21	✓
4	Высокая	CVE-2026-25990	Pillow	Сетевой	ACE	2026-02-20	✓
5	Высокая	CVE-2026-2045	GIMP	Локальный	ACE	2026-02-20	✓
6	Высокая	CVE-2026-2047	GIMP	Локальный	ACE	2026-02-20	✓
7	Высокая	CVE-2026-2048	GIMP	Локальный	ACE	2026-02-20	✓
8	Высокая	CVE-2026-2044	GIMP	Локальный	ACE	2026-02-20	✓
9	Высокая	CVE-2026-20626	Apple macOS Tahoe	Локальный	PE	2026-02-11	✓
10	Высокая	CVE-2026-20649	Apple macOS Tahoe	Сетевой	OSI	2026-02-11	✓
11	Высокая	CVE-2026-20700	Apple macOS Tahoe	Локальный	ACE	2026-02-11	✓
12	Высокая	CVE-2025-43529	Apple macOS Tahoe	Сетевой	ACE	2026-02-11	✓
13	Высокая	CVE-2025-14174	Apple macOS Tahoe	Сетевой	ACE	2026-02-11	✓

14	Высокая	CVE-2026-20650	Apple macOS Tahoe	Сетевой	DoS	2026-02-11	✓
15	Высокая	CVE-2026-20652	Apple macOS Tahoe	Сетевой	DoS	2026-02-11	✓
16	Высокая	CVE-2026-20610	Apple macOS Tahoe	Локальный	PE	2026-02-11	✓
17	Высокая	CVE-2026-20658	Apple macOS Tahoe	Локальный	PE	2026-02-11	✓
18	Критическая	CVE-2026-20677	Apple macOS Tahoe и Sonoma	Сетевой	SB	2026-02-11	✓
19	Высокая	CVE-2026-20667	Apple macOS Tahoe и Sonoma	Локальный	PE	2026-02-11	✓
20	Высокая	CVE-2025-59375	Apple macOS Tahoe и Sonoma	Сетевой	DoS	2026-02-11	✓
21	Высокая	CVE-2026-20620	Apple macOS Tahoe и Sonoma	Локальный	OSI	2026-02-11	✓
22	Высокая	CVE-2026-20615	Apple macOS Tahoe и Sonoma	Локальный	PE	2026-02-11	✓
23	Высокая	CVE-2026-20660	Apple macOS Tahoe и Sonoma	Сетевой	PE	2026-02-11	✓
24	Высокая	CVE-2025-43402	Apple macOS Sonoma	Локальный	PE	2026-02-11	✓
25	Высокая	CVE-2025-46290	Apple macOS Sonoma	Сетевой	DoS	2026-02-11	✓
26	Высокая	CVE-2026-20614	Apple macOS Tahoe и Sonoma	Локальный	PE	2026-02-11	✓
27	Высокая	CVE-2026-2650	Google Chrome	Сетевой	ACE	2026-02-19	✓
28	Высокая	CVE-2026-2649	Google Chrome	Сетевой	ACE	2026-02-19	✓

29	Высокая	CVE-2026-2648	Google Chrome	Сетевой	ACE	2026-02-19	✓
30	Высокая	CVE-2026-2630	Tenable Security Center	Сетевой	ACE	2026-02-18	✓
31	Высокая	CVE-2025-14180	Tenable Security Center	Сетевой	DoS	2026-02-18	✓
32	Высокая	CVE-2026-2314	Microsoft Edge	Сетевой	ACE	2026-02-18	✓
33	Высокая	CVE-2026-2319	Microsoft Edge	Сетевой	SB	2026-02-18	✓
34	Высокая	CVE-2026-2313	Microsoft Edge	Сетевой	ACE	2026-02-18	✓
35	Высокая	CVE-2026-2441	Microsoft Edge	Сетевой	ACE	2026-02-18	✓
36	Высокая	CVE-2026-0875	Autodesk Shared Components	Локальный	ACE	2026-02-19	✓
37	Высокая	CVE-2026-0874	Autodesk Shared Components	Локальный	ACE	2026-02-19	✓
38	Критическая	CVE-2026-22769	Dell RecoverPoint for Virtual Machines	Сетевой	ACE	2026-02-18	✓
39	Критическая	CVE-2025-49796	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-02-17	✓
40	Критическая	CVE-2025-49794	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-02-17	✓
41	Высокая	CVE-2025-48384	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2026-02-17	✓
42	Высокая	CVE-2025-48060	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-02-17	✓

43	Высокая	CVE-2025-47273	Ansible Automation Platform 2.5 packages	Сетевой	OSI	2026-02-17	✓
44	Высокая	CVE-2025-46835	Ansible Automation Platform 2.5 packages	Локальный	OSI	2026-02-17	✓
45	Высокая	CVE-2025-27614	Ansible Automation Platform 2.5 packages	Локальный	OSI	2026-02-17	✓
46	Высокая	CVE-2025-6021	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2026-02-17	✓
47	Высокая	CVE-2025-6020	Ansible Automation Platform 2.5 packages	Локальный	ACE	2026-02-17	✓
48	Критическая	CVE-2025-4517	Ansible Automation Platform 2.5 packages	Сетевой	WLF	2026-02-17	✓
49	Высокая	CVE-2025-4330	Ansible Automation Platform 2.5 packages	Сетевой	OAF	2026-02-17	✓
50	Высокая	CVE-2025-4138	Ansible Automation Platform 2.5 packages	Сетевой	OAF	2026-02-17	✓
51	Критическая	CVE-2024-54661	Ansible Automation Platform 2.5 packages	Сетевой	OAF	2026-02-17	✓
52	Высокая	CVE-2024-53920	Ansible Automation Platform 2.5 packages	Локальный	ACE	2026-02-17	✓
53	Критическая	CVE-2024-52533	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2026-02-17	✓
54	Высокая	CVE-2024-52006	Ansible Automation Platform 2.5 packages	Сетевой	OSI	2026-02-17	✓

55	Высокая	CVE-2019-17543	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2026-02-17	✓
56	Высокая	CVE-2026-2034	Sante DICOM Viewer Pro	Локальный	ACE	2026-02-17	✓
57	Высокая	CVE-2025-62707	pypdf	Сетевой	DoS	2026-02-12	✓
58	Высокая	CVE-2026-23720	Siemens Simcenter Femap and Nastran	Локальный	OSI	2026-02-12	✓
59	Высокая	CVE-2026-23719	Siemens Simcenter Femap and Nastran	Локальный	ACE	2026-02-12	✓
60	Высокая	CVE-2026-23718	Siemens Simcenter Femap and Nastran	Локальный	OSI	2026-02-12	✓
61	Высокая	CVE-2026-23717	Siemens Simcenter Femap and Nastran	Локальный	OSI	2026-02-12	✓
62	Высокая	CVE-2026-23716	Siemens Simcenter Femap and Nastran	Локальный	OSI	2026-02-12	✓
63	Высокая	CVE-2026-23715	Siemens Simcenter Femap and Nastran	Локальный	ACE	2026-02-12	✓
64	Высокая	CVE-2026-2321	Google Chrome	Сетевой	OSI	2026-02-12	✓
65	Высокая	CVE-2026-2319	Google Chrome	Сетевой	SB	2026-02-12	✓
66	Высокая	CVE-2026-2315	Google Chrome	Сетевой	OSI	2026-02-12	✓
67	Высокая	CVE-2026-2314	Google Chrome	Сетевой	ACE	2026-02-12	✓
68	Высокая	CVE-2026-2313	Google Chrome	Сетевой	ACE	2026-02-12	✓
69	Критическая	CVE-2025-66277	QNAP QTS and QuTS hero	Сетевой	PE	2026-02-12	✓

70	Высокая	CVE-2026-0900	Prisma Access Browser	Сетевой	OSI	2026-02-11	✓
71	Высокая	CVE-2026-0902	Prisma Access Browser	Сетевой	OSI	2026-02-11	✓
72	Критическая	CVE-2026-0905	Prisma Access Browser	Сетевой	OSI	2026-02-11	✓
73	Критическая	CVE-2026-0906	Prisma Access Browser	Сетевой	XSS\CSS	2026-02-11	✓
74	Высокая	CVE-2026-0899	Prisma Access Browser	Сетевой	ACE	2026-02-11	✓
75	Критическая	CVE-2026-0907	Prisma Access Browser	Сетевой	XSS\CSS	2026-02-11	✓
76	Высокая	CVE-2026-1861	Prisma Access Browser	Сетевой	ACE	2026-02-11	✓
77	Высокая	CVE-2026-1862	Prisma Access Browser	Сетевой	ACE	2026-02-11	✓
78	Высокая	CVE-2026-0908	Prisma Access Browser	Сетевой	DoS	2026-02-11	✓
79	Высокая	CVE-2026-1761	libsoup	Сетевой	ACE	2026-02-11	✗
80	Высокая	CVE-2026-0719	libsoup	Сетевой	ACE	2026-02-11	✗
81	Высокая	CVE-2026-0958	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	DoS	2026-02-11	✓
82	Высокая	CVE-2025-8099	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	DoS	2026-02-11	✓
83	Высокая	CVE-2025-7659	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	OSI	2026-02-11	✓

84	Высокая	CVE-2026-21330	Adobe After Effects	Локальный	ACE	2026-02-10	✓
85	Высокая	CVE-2026-21320	Adobe After Effects	Локальный	ACE	2026-02-10	✓
86	Высокая	CVE-2026-21321	Adobe After Effects	Локальный	ACE	2026-02-10	✓
87	Высокая	CVE-2026-21322	Adobe After Effects	Локальный	OSI	2026-02-10	✓
88	Высокая	CVE-2026-21323	Adobe After Effects	Локальный	ACE	2026-02-10	✓
89	Высокая	CVE-2026-21324	Adobe After Effects	Локальный	OSI	2026-02-10	✓
90	Высокая	CVE-2026-21325	Adobe After Effects	Локальный	OSI	2026-02-10	✓
91	Высокая	CVE-2026-21326	Adobe After Effects	Локальный	ACE	2026-02-10	✓
92	Высокая	CVE-2026-21327	Adobe After Effects	Локальный	ACE	2026-02-10	✓
93	Высокая	CVE-2026-21318	Adobe After Effects	Локальный	ACE	2026-02-10	✓
94	Высокая	CVE-2026-21328	Adobe After Effects	Локальный	ACE	2026-02-10	✓
95	Высокая	CVE-2026-21351	Adobe After Effects	Локальный	ACE	2026-02-10	✓
96	Средняя	CVE-2026-21319	Adobe After Effects	Локальный	OSI	2026-02-10	✓
97	Высокая	CVE-2026-21329	Adobe After Effects	Локальный	ACE	2026-02-10	✓
98	Высокая	CVE-2026-21523	Microsoft GitHub Copilot and Visual Studio	Сетевой	ACE	2026-02-10	✓

99	Высокая	CVE-2026-21257	Microsoft GitHub Copilot and Visual Studio	Сетевой	ACE	2026-02-10	✓
100	Высокая	CVE-2026-21256	Microsoft GitHub Copilot and Visual Studio	Сетевой	ACE	2026-02-10	✓
101	Высокая	CVE-2026-21312	Adobe Audition	Локальный	ACE	2026-02-10	✓
102	Высокая	CVE-2026-21347	Adobe Bridge	Локальный	ACE	2026-02-10	✓
103	Высокая	CVE-2026-21346	Adobe Bridge	Локальный	ACE	2026-02-10	✓
104	Высокая	CVE-2026-21353	Adobe DNG Software Development Kit (SDK)	Локальный	ACE	2026-02-10	✓
105	Высокая	CVE-2026-21352	Adobe DNG Software Development Kit (SDK)	Локальный	ACE	2026-02-10	✓
106	Высокая	CVE-2026-21357	Adobe InDesign	Локальный	ACE	2026-02-10	✓
107	Высокая	CVE-2026-21516	Microsoft GitHub Copilot for Jetbrains	Сетевой	ACE	2026-02-10	✓
108	Высокая	CVE-2026-21349	Lightroom Classic	Локальный	ACE	2026-02-10	✓
109	Высокая	CVE-2026-21335	Adobe Substance 3D Designer	Локальный	ACE	2026-02-10	✓
110	Высокая	CVE-2026-21334	Adobe Substance 3D Designer	Локальный	ACE	2026-02-10	✓
111	Высокая	CVE-2026-21345	Adobe Substance 3D Stager	Локальный	OSI	2026-02-10	✓
112	Высокая	CVE-2026-21344	Adobe Substance 3D Stager	Локальный	OSI	2026-02-10	✓

113	Высокая	CVE-2026-21343	Adobe Substance 3D Stager	Локальный	OSI	2026-02-10	✓
114	Высокая	CVE-2026-21342	Adobe Substance 3D Stager	Локальный	ACE	2026-02-10	✓
115	Высокая	CVE-2026-21341	Adobe Substance 3D Stager	Локальный	ACE	2026-02-10	✓
116	Высокая	CVE-2026-21259	Microsoft Excel	Локальный	PE	2026-02-10	✓
117	Критическая	CVE-2026-21531	Microsoft Azure SDK for Python	Сетевой	ACE	2026-02-10	✓
118	Высокая	CVE-2026-1603	Ivanti Endpoint Manager	Сетевой	SB	2026-02-10	✓
119	Высокая	CVE-2026-21228	Microsoft Azure Local	Сетевой	ACE	2026-02-10	✓
120	Высокая	CVE-2026-21519	Microsoft Desktop Window Manager	Локальный	ACE	2026-02-10	✓
121	Высокая	CVE-2026-21533	Microsoft Windows Remote Desktop	Локальный	PE	2026-02-10	✓
122	Высокая	CVE-2026-21513	Microsoft MSHTML Framework	Сетевой	ACE	2026-02-10	✓
123	Высокая	CVE-2026-21510	Windows Shell	Сетевой	ACE	2026-02-10	✓
124	Высокая	CVE-2026-21514	Microsoft Word	Локальный	ACE	2026-02-10	✓
125	Высокая	CVE-2026-22153	FortiOS	Сетевой	SB	2026-02-10	✓
126	Критическая	CVE-2026-22854	FreeRDP	Сетевой	ACE	2026-02-10	✓
127	Критическая	CVE-2026-22855	FreeRDP	Сетевой	ACE	2026-02-10	✓

128	Высокая	CVE-2026-22856	FreeRDP	Сетевой	ACE	2026-02-10	✓
129	Критическая	CVE-2026-22857	FreeRDP	Сетевой	ACE	2026-02-10	✓
130	Критическая	CVE-2026-22858	FreeRDP	Сетевой	DoS	2026-02-10	✓
131	Критическая	CVE-2026-22859	FreeRDP	Сетевой	DoS	2026-02-10	✓
132	Критическая	CVE-2026-22853	FreeRDP	Сетевой	ACE	2026-02-10	✓
133	Критическая	CVE-2026-22852	FreeRDP	Сетевой	ACE	2026-02-10	✓
134	Высокая	CVE-2026-24682	FreeRDP	Сетевой	ACE	2026-02-10	✓
135	Высокая	CVE-2026-24683	FreeRDP	Сетевой	ACE	2026-02-10	✓
136	Высокая	CVE-2026-24676	FreeRDP	Сетевой	ACE	2026-02-10	✓
137	Критическая	CVE-2026-24677	FreeRDP	Сетевой	ACE	2026-02-10	✓
138	Высокая	CVE-2026-24678	FreeRDP	Сетевой	ACE	2026-02-10	✓
139	Высокая	CVE-2026-24684	FreeRDP	Сетевой	ACE	2026-02-10	✓
140	Критическая	CVE-2026-24679	FreeRDP	Сетевой	ACE	2026-02-10	✓
141	Высокая	CVE-2026-24681	FreeRDP	Сетевой	ACE	2026-02-10	✓
142	Высокая	CVE-2026-24675	FreeRDP	Сетевой	ACE	2026-02-10	✓

143	Высокая	CVE-2026-24491	FreeRDP	Сетевой	ACE	2026-02-10	✓
144	Высокая	CVE-2026-24680	FreeRDP	Сетевой	ACE	2026-02-10	✓
145	Высокая	CVE-2026-23948	FreeRDP	Сетевой	DoS	2026-02-10	✓
146	Высокая	CVE-2025-64175	gogs	Сетевой	SB	2026-02-09	✓
147	Высокая	CVE-2026-24135	gogs	Сетевой	OAF	2026-02-09	✓
148	Критическая	CVE-2025-64111	gogs	Сетевой	ACE	2026-02-09	✓
149	Критическая	CVE-2026-25848	JetBrains Hub	Сетевой	OSI	2026-02-09	✓
150	Высокая	CVE-2026-25055	n8n	Сетевой	WLF	2026-02-06	✓
151	Высокая	CVE-2026-1862	Microsoft Edge	Сетевой	ACE	2026-02-06	✓
152	Высокая	CVE-2026-1861	Microsoft Edge	Сетевой	ACE	2026-02-06	✓
153	Высокая	CVE-2026-0659	Autodesk Arnold	Локальный	ACE	2026-02-05	✓
154	Высокая	CVE-2026-0662	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓
155	Высокая	CVE-2026-0660	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓
156	Высокая	CVE-2026-0536	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓
157	Высокая	CVE-2026-0537	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓

158	Высокая	CVE-2026-0661	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓
159	Высокая	CVE-2026-0538	Autodesk 3ds Max	Локальный	ACE	2026-02-05	✓
160	Высокая	CVE-2026-0915	GNU C Library (glibc)	Сетевой	OSI	2026-02-04	✓
161	Высокая	CVE-2026-0861	GNU C Library (glibc)	Локальный	ACE	2026-02-04	✓
162	Высокая	CVE-2025-15281	GNU C Library (glibc)	Сетевой	DoS	2026-02-04	✓
163	Критическая	CVE-2025-11953	React Native Community CLI	Сетевой	ACE	2026-02-03	✓
164	Высокая	CVE-2026-1285	Django	Сетевой	DoS	2026-02-03	✓
165	Высокая	CVE-2025-14550	Django	Сетевой	DoS	2026-02-03	✓
166	Не определено	CVE-2026-1498	WatchGuard Firebox Fireware OS	Не определено	SB	2026-01-30	✓
167	Высокая	CVE-2025-66276	QNAP QTS	Сетевой	ACE	2026-01-30	✓
168	Высокая	CVE-2026-22258	Suricata	Сетевой	DoS	2026-01-28	✓
169	Высокая	CVE-2026-22260	Suricata	Сетевой	DoS	2026-01-28	✓
170	Высокая	CVE-2026-22259	Suricata	Сетевой	DoS	2026-01-28	✓
171	Высокая	CVE-2025-69421	OpenSSL	Сетевой	DoS	2026-01-27	✓
172	Высокая	CVE-2025-69420	OpenSSL	Сетевой	DoS	2026-01-27	✓

173	Критическая	CVE-2025-15467	OpenSSL	Сетевой	ACE	2026-01-27	✓
174	Критическая	CVE-2025-68670	xrdp	Сетевой	ACE	2026-01-28	✓
175	Высокая	CVE-2026-24869	Mozilla Firefox	Сетевой	ACE	2026-01-27	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-2649

Идентификатор программной ошибки: CWE-472 Возможность изменения извне предположительно неизменяемых веб-параметров

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.65

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-21 / 2026-02-21

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2650
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2648
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2649

2	**Краткое описание:** Выполнение произвольного кода в Microsoft Edge **Идентификатор уязвимости:** CVE-2026-2648 **Идентификатор программной ошибки:** CWE-122 Переполнение буфера в динамической памяти **Уязвимый продукт:** Microsoft Edge: 100.0.1185.29 - 145.0.3800.65 **Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Оценка CVSSv4:** Не определено **Вектор атаки:** Сетевой **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2026-02-21 / 2026-02-21 **Ссылки на источник:** • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2650 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2648 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2649

3

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-2650

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.65

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-21 / 2026-02-21

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2650
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2648
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2649

4

Краткое описание: Выполнение произвольного кода в Pillow

Идентификатор уязвимости: CVE-2026-25990

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Pillow: 10.3.0 - 12.1.0

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

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-20 / 2026-02-20

Ссылки на источник:

- https://github.com/python-pillow/Pillow/security/advisories/GHSA-cfh3-3jmp-rvhc

5

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2026-2045

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Gimp: до 3.0.8

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-20 / 2026-02-20

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-118/
- https://www.zerodayinitiative.com/advisories/ZDI-26-121/
- https://www.zerodayinitiative.com/advisories/ZDI-26-120/
- https://www.zerodayinitiative.com/advisories/ZDI-26-119/

6

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2026-2047

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

Уязвимый продукт: Gimp: до 3.0.8

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-20 / 2026-02-20

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-118/
- https://www.zerodayinitiative.com/advisories/ZDI-26-121/
- https://www.zerodayinitiative.com/advisories/ZDI-26-120/
- https://www.zerodayinitiative.com/advisories/ZDI-26-119/

7

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2026-2048

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Gimp: до 3.0.8

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-20 / 2026-02-20

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-118/
- https://www.zerodayinitiative.com/advisories/ZDI-26-121/
- https://www.zerodayinitiative.com/advisories/ZDI-26-120/
- https://www.zerodayinitiative.com/advisories/ZDI-26-119/

8

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2026-2044

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Gimp: до 3.0.8

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-20 / 2026-02-20

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-118/
- https://www.zerodayinitiative.com/advisories/ZDI-26-121/
- https://www.zerodayinitiative.com/advisories/ZDI-26-120/
- https://www.zerodayinitiative.com/advisories/ZDI-26-119/

9

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20626

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

10

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20649

Идентификатор программной ошибки: CWE-377 Уязвимости, связанные с небезопасными временными файлами

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Непреднамеренное предоставление чувствительной 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

11

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20700

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

12

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43529

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

13

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-14174

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

14

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20650

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

15

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20652

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

16

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20610

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

17

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2026-20658

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348

18

Краткое описание: Обход безопасности в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20677

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Использование ситуации гонки (race condition) в системе.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 9.0 AV:N/AC:H/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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

19

Краткое описание: Повышение привилегий в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20667

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

20

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2025-59375

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

21

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20620

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Чтение за пределами буфера.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

22

Краткое описание: Повышение привилегий в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20615

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

23

Краткое описание: Повышение привилегий в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20660

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

24

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43402

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126350

25

Краткое описание: Отказ в обслуживании в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-46290

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126350

26

Краткое описание: Повышение привилегий в Apple macOS Tahoe и Sonoma

Идентификатор уязвимости: CVE-2026-20614

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

Уязвимый продукт: macOS: 26.0 RC - 26.2 25C56
macOS: 14.0 23A344 - 14.8.3 23J220

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://support.apple.com/en-us/126348
- https://support.apple.com/en-us/126350

27

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-2650

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.77

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-19 / 2026-02-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_18.html
- https://crbug.com/477033835https://crbug.com/481074858https://crbug.com/476461867

28

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-2649

Идентификатор программной ошибки: CWE-472 Возможность изменения извне предположительно неизменяемых веб-параметров

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.77

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-19 / 2026-02-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_18.html
- https://crbug.com/477033835https://crbug.com/481074858https://crbug.com/476461867

29

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-2648

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.77

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-19 / 2026-02-19

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_18.html
- https://crbug.com/477033835https://crbug.com/481074858https://crbug.com/476461867

30

Краткое описание: Выполнение произвольного кода в Tenable Security Center

Идентификатор уязвимости: CVE-2026-2630

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

Уязвимый продукт: SecurityCenter: 6.5.1 - SC-202509.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 7.0 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-18 / 2026-02-18

Ссылки на источник:

- https://www.tenable.com/security/tns-2026-06

31

Краткое описание: Отказ в обслуживании в Tenable Security Center

Идентификатор уязвимости: CVE-2025-14180

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: SecurityCenter: 6.5.1 - SC-202509.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 8.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-18 / 2026-02-18

Ссылки на источник:

- https://www.tenable.com/security/tns-2026-06

32

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-2314

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 144.0.3719.115

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-18 / 2026-02-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2320
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2441
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2323
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-0102
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2318
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2317
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2313
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2319
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2316
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2314
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2322

33	**Краткое описание:** Обход безопасности в Microsoft Edge **Идентификатор уязвимости:** CVE-2026-2319 **Идентификатор программной ошибки:** CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки) **Уязвимый продукт:** Microsoft Edge: 100.0.1185.29 - 144.0.3719.115 **Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты **Способ эксплуатации:** Открытие пользователем специально созданной вредоносной веб-страницы. **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: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:** 2026-02-18 / 2026-02-20 **Ссылки на источник:** • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2320 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2441 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2323 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-0102 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2318 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2317 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2313 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2319 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2316 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2314 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2322

34

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-2313

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 144.0.3719.115

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-18 / 2026-02-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2320
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2441
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2323
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-0102
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2318
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2317
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2313
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2319
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2316
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2314
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2322

35

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-2441

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 144.0.3719.115

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-18 / 2026-02-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2320
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2441
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2323
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-0102
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2318
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2317
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2313
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2319
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2316
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2314
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-2322

36

Краткое описание: Выполнение произвольного кода в Autodesk Shared Components

Идентификатор уязвимости: CVE-2026-0875

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk Shared Components: 2026.0 - 2026.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-19 / 2026-02-19

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0004https://www.zerodayinitiative.com/advisories/ZDI-26-106/https://www.zerodayinitiative.com/advisories/ZDI-26-107/

37

Краткое описание: Выполнение произвольного кода в Autodesk Shared Components

Идентификатор уязвимости: CVE-2026-0874

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk Shared Components: 2026.0 - 2026.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-19 / 2026-02-19

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0004https://www.zerodayinitiative.com/advisories/ZDI-26-106/https://www.zerodayinitiative.com/advisories/ZDI-26-107/

38

Краткое описание: Выполнение произвольного кода в Dell RecoverPoint for Virtual Machines

Идентификатор уязвимости: CVE-2026-22769

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: RecoverPoint for Virtual Machines: 5.3 SP2 - 6.0 SP3 P1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование жестко закодированных учетных 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: 2026-02-18 / 2026-02-18

Ссылки на источник:

- https://www.dell.com/support/kbdoc/nl-nl/000426773/dsa-2026-079https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day/

39

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-49796

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

40

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-49794

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

41

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-48384

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

42

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-48060

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 7.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

43

Краткое описание: Получение конфиденциальной информации в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-47273

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 7.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

44

Краткое описание: Получение конфиденциальной информации в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-46835

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.5 AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

45

Краткое описание: Получение конфиденциальной информации в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-27614

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Наличие встроенной вредоносной функциональности в коде приложения

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.6 AV:L/AC:L/PR:N/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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

46

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-6021

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

47

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-6020

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование ситуации гонки (race condition) в системе.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

48

Краткое описание: Запись локальных файлов в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-4517

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

49

Краткое описание: Перезапись произвольных файлов в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-4330

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

50

Краткое описание: Перезапись произвольных файлов в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-4138

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

51

Краткое описание: Перезапись произвольных файлов в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2024-54661

Идентификатор программной ошибки: CWE-61 Уязвимости, связанные с символическими ссылками UNIX

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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: 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

52

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2024-53920

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

53

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2024-52533

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

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

54

Краткое описание: Получение конфиденциальной информации в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2024-52006

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

55

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2019-17543

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:12791

56

Краткое описание: Выполнение произвольного кода в Sante DICOM Viewer Pro

Идентификатор уязвимости: CVE-2026-2034

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

Уязвимый продукт: DICOM Viewer Pro: до 14.2.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-17 / 2026-02-17

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-104/

57

Краткое описание: Отказ в обслуживании в pypdf

Идентификатор уязвимости: CVE-2025-62707

Идентификатор программной ошибки: CWE-834 Излишние итерации

Уязвимый продукт: PyPDF: 1.17 - 6.1.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 6.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://github.com/py-pdf/pypdf/commit/f2864d6dd9bac7cecd3f4f54308b25ebbfa178f8
- https://github.com/py-pdf/pypdf/pull/3501
- https://github.com/py-pdf/pypdf/releases/tag/6.1.3
- https://github.com/py-pdf/pypdf/security/advisories/GHSA-vr63-x8vc-m265

58

Краткое описание: Получение конфиденциальной информации в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23720

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

59

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23719

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

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

60

Краткое описание: Получение конфиденциальной информации в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23718

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

61

Краткое описание: Получение конфиденциальной информации в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23717

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

62

Краткое описание: Получение конфиденциальной информации в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23716

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

63

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap and Nastran

Идентификатор уязвимости: CVE-2026-23715

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Simcenter Femap: до 2512
Simcenter Nastran: до 2512

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

64

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-2321

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.26

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html
- https://crbug.com/467297219
- https://crbug.com/478560268
- https://crbug.com/479242793
- https://crbug.com/422531206
- https://crbug.com/464173573
- https://crbug.com/363930141
- https://crbug.com/40071155
- https://crbug.com/435684924
- https://crbug.com/461877477
- https://crbug.com/470928605
- https://crbug.com/467442136

65

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-2319

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.26

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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: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: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html
- https://crbug.com/467297219
- https://crbug.com/478560268
- https://crbug.com/479242793
- https://crbug.com/422531206
- https://crbug.com/464173573
- https://crbug.com/363930141
- https://crbug.com/40071155
- https://crbug.com/435684924
- https://crbug.com/461877477
- https://crbug.com/470928605

- https://crbug.com/467442136

66

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-2315

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.26

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html
- https://crbug.com/467297219
- https://crbug.com/478560268
- https://crbug.com/479242793
- https://crbug.com/422531206
- https://crbug.com/464173573
- https://crbug.com/363930141
- https://crbug.com/40071155
- https://crbug.com/435684924
- https://crbug.com/461877477
- https://crbug.com/470928605
- https://crbug.com/467442136

67

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-2314

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.26

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html
- https://crbug.com/467297219
- https://crbug.com/478560268
- https://crbug.com/479242793
- https://crbug.com/422531206
- https://crbug.com/464173573
- https://crbug.com/363930141
- https://crbug.com/40071155
- https://crbug.com/435684924
- https://crbug.com/461877477
- https://crbug.com/470928605
- https://crbug.com/467442136

68

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-2313

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.26

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html
- https://crbug.com/467297219
- https://crbug.com/478560268
- https://crbug.com/479242793
- https://crbug.com/422531206
- https://crbug.com/464173573
- https://crbug.com/363930141
- https://crbug.com/40071155
- https://crbug.com/435684924
- https://crbug.com/461877477
- https://crbug.com/470928605
- https://crbug.com/467442136

69

Краткое описание: Повышение привилегий в QNAP QTS and QuTS hero

Идентификатор уязвимости: CVE-2025-66277

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

Уязвимый продукт: QNAP QTS: до 5.2.8.3350 20251216
QuTS hero: до h5.2.8.3350 build 20251216

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 9.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-12 / 2026-02-12

Ссылки на источник:

- https://www.qnap.com/en/security-advisory/qsa-26-05

70

Краткое описание: Получение конфиденциальной информации в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0900

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

71

Краткое описание: Получение конфиденциальной информации в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0902

Идентификатор программной ошибки: CWE-474 Использование функции с непоследовательной реализацией

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

72

Краткое описание: Получение конфиденциальной информации в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0905

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

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

73

Краткое описание: Межсайтовый скриптинг в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0906

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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: 9.8 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

74

Краткое описание: Выполнение произвольного кода в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0899

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

75

Краткое описание: Межсайтовый скриптинг в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0907

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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: 9.8 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

76

Краткое описание: Выполнение произвольного кода в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-1861

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

77

Краткое описание: Выполнение произвольного кода в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-1862

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

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

78

Краткое описание: Отказ в обслуживании в Prisma Access Browser

Идентификатор уязвимости: CVE-2026-0908

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Prisma Access Browser: до 144.27.7.133

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://security.paloaltonetworks.com/PAN-SA-2026-0002

Краткое описание: Выполнение произвольного кода в libsoup

Идентификатор уязвимости: CVE-2026-1761

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: libsoup: 2.0 - 3.6.5

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

79

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://bugzilla.redhat.com/show_bug.cgi?id=2427906
- https://gitlab.gnome.org/GNOME/libsoup/-/issues/477
- https://access.redhat.com/security/cve/CVE-2026-1761
- https://bugzilla.redhat.com/show_bug.cgi?id=2435961

80

Краткое описание: Выполнение произвольного кода в libsoup

Идентификатор уязвимости: CVE-2026-0719

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: libsoup: 2.0 - 3.6.5

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://bugzilla.redhat.com/show_bug.cgi?id=2427906
- https://gitlab.gnome.org/GNOME/libsoup/-/issues/477https://access.redhat.com/security/cve/CVE-2026-1761
- https://bugzilla.redhat.com/show_bug.cgi?id=2435961

81

Краткое описание: Отказ в обслуживании в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2026-0958

Идентификатор программной ошибки: CWE-436 Конфликт интерпретации

Уязвимый продукт: GitLab Enterprise Edition: 8.0.0 - 18.8.3
Gitlab Community Edition: 8.0 - 18.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://about.gitlab.com/releases/2026/02/10/patch-release-gitlab-18-8-4-released/

82

Краткое описание: Отказ в обслуживании в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-8099

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

Уязвимый продукт: GitLab Enterprise Edition: 8.0.0 - 18.8.3
Gitlab Community Edition: 8.0 - 18.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://about.gitlab.com/releases/2026/02/10/patch-release-gitlab-18-8-4-released/

83

Краткое описание: Получение конфиденциальной информации в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-7659

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

Уязвимый продукт: GitLab Enterprise Edition: 8.0.0 - 18.8.3
Gitlab Community Edition: 8.0 - 18.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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: 8.0 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://about.gitlab.com/releases/2026/02/10/patch-release-gitlab-18-8-4-released/

84

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21330

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

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

85

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21320

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

86

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21321

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

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

87

Краткое описание: Получение конфиденциальной информации в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21322

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

88

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21323

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

89

Краткое описание: Получение конфиденциальной информации в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21324

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

90

Краткое описание: Получение конфиденциальной информации в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21325

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

91

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21326

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

92

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21327

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

93

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21318

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

94

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21328

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

95

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21351

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

96

Краткое описание: Получение конфиденциальной информации в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21319

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

97

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2026-21329

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 22.0 - 25.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/after_effects/apsb26-15.html

98

Краткое описание: Выполнение произвольного кода в Microsoft GitHub Copilot and Visual Studio

Идентификатор уязвимости: CVE-2026-21523

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

Уязвимый продукт: Visual Studio Code: 1.0.0 - 14
Visual Studio: 2022 version 17.14 - 2022 version 18.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование ситуации гонки (race condition) в системе.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-19

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21518
- https://github.com/microsoft/vscode/security/advisories/GHSA-6xq8-9qf3-p6qv
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21256
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21257
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21523
- https://github.com/microsoft/vscode/security/advisories/GHSA-3pwg-f3hj-wp8p

99

Краткое описание: Выполнение произвольного кода в Microsoft GitHub Copilot and Visual Studio

Идентификатор уязвимости: CVE-2026-21257

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Visual Studio Code: 1.0.0 - 14
Visual Studio: 2022 version 17.14 - 2022 version 18.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-19

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21518
- https://github.com/microsoft/vscode/security/advisories/GHSA-6xq8-9qf3-p6qv
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21256
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21257
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21523
- https://github.com/microsoft/vscode/security/advisories/GHSA-3pwg-f3hj-wp8p

100

Краткое описание: Выполнение произвольного кода в Microsoft GitHub Copilot and Visual Studio

Идентификатор уязвимости: CVE-2026-21256

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Visual Studio Code: 1.0.0 - 14
Visual Studio: 2022 version 17.14 - 2022 version 18.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-19

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21518
- https://github.com/microsoft/vscode/security/advisories/GHSA-6xq8-9qf3-p6qv
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21256
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21257
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21523
- https://github.com/microsoft/vscode/security/advisories/GHSA-3pwg-f3hj-wp8p

101

Краткое описание: Выполнение произвольного кода в Adobe Audition

Идентификатор уязвимости: CVE-2026-21312

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Audition: 22.0 - 25.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/audition/apsb26-14.html

102

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2026-21347

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

Уязвимый продукт: Adobe Bridge: 15.0 - 16.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/bridge/apsb26-21.html

103

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2026-21346

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Bridge: 15.0 - 16.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/bridge/apsb26-21.html

104

Краткое описание: Выполнение произвольного кода в Adobe DNG Software Development Kit (SDK)

Идентификатор уязвимости: CVE-2026-21353

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

Уязвимый продукт: Adobe DNG Software Development Kit (SDK): 1.4 (2012) - 1.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/dng-sdk/apsb26-23.html

105

Краткое описание: Выполнение произвольного кода в Adobe DNG Software Development Kit (SDK)

Идентификатор уязвимости: CVE-2026-21352

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe DNG Software Development Kit (SDK): 1.4 (2012) - 1.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/dng-sdk/apsb26-23.html

106

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-21357

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: 20.0 - 2015

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-17.html

107

Краткое описание: Выполнение произвольного кода в Microsoft GitHub Copilot for Jetbrains

Идентификатор уязвимости: CVE-2026-21516

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: GitHub Copilot Plugin for JetBrains IDEs: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21516

108

Краткое описание: Выполнение произвольного кода в Lightroom Classic

Идентификатор уязвимости: CVE-2026-21349

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Lightroom Classic: до 14.5.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/lightroom/apsb26-06.html

109

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Designer

Идентификатор уязвимости: CVE-2026-21335

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: 15.0.0 - 15.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-19.html

110

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Designer

Идентификатор уязвимости: CVE-2026-21334

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: 15.0.0 - 15.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-19.html

111

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-21345

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-20.html

112

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-21344

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-20.html

113

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-21343

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-20.html

114

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-21342

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-20.html

115

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-21341

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-20.html

116

Краткое описание: Повышение привилегий в Microsoft Excel

Идентификатор уязвимости: CVE-2026-21259

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Office Online Server : все версии
Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21259https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21261https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21258

117

Краткое описание: Выполнение произвольного кода в Microsoft Azure SDK for Python

Идентификатор уязвимости: CVE-2026-21531

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Azure AI Language Authoring: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21531

118

Краткое описание: Обход безопасности в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2026-1603

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

Уязвимый продукт: Endpoint Manager: 2022 - 2024 SU4 SR1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса 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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-19

Ссылки на источник:

- https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024https://www.zerodayinitiative.com/advisories/ZDI-26-079/https://www.zerodayinitiative.com/advisories/ZDI-26-080/

119

Краткое описание: Выполнение произвольного кода в Microsoft Azure Local

Идентификатор уязвимости: CVE-2026-21228

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Azure Local: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка сертификатов.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21228

120

Краткое описание: Выполнение произвольного кода в Microsoft Desktop Window Manager

Идентификатор уязвимости: CVE-2026-21519

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

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7623
Windows Server: 2012 Gold - 2025 10.0.26100.32230

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21519

121

Краткое описание: Повышение привилегий в Microsoft Windows Remote Desktop

Идентификатор уязвимости: CVE-2026-21533

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7623
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32230

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533

Краткое описание: Выполнение произвольного кода в Microsoft MSHTML Framework

Идентификатор уязвимости: CVE-2026-21513

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7623
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32230
Microsoft Internet Explorer: 11 - 11.1790.17763.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513

123

Краткое описание: Выполнение произвольного кода в Windows Shell

Идентификатор уязвимости: CVE-2026-21510

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7623
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32230

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21510

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-21514

Идентификатор программной ошибки: CWE-807 Использование недоверенных входных данных при обеспечении безопасности

Уязвимый продукт: Microsoft Office: 2024
Microsoft Office for macOS: до 16.106.26020821 16.106.26020821
Microsoft 365 Apps for Enterprise: до 16.0.19725.20058

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514

125

Краткое описание: Обход безопасности в FortiOS

Идентификатор уязвимости: CVE-2026-22153

Идентификатор программной ошибки: CWE-305 Обход аутентификации с помощью стороннего недостатка

Уязвимый продукт: FortiOS: 7.6.0 - 7.6.4

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса 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: 8.1 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: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-1052

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22854

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

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

126 **Оценка CVSSv4:** 6.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5ch
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhv
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmf
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22855

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

127 **Оценка CVSSv4:** 5.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5ch
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhv
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmf
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22856

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

128

Оценка CVSSv4: 6.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22857

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

129 **Оценка CVSSv4:** 6.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-22858

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

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

130 **Оценка CVSSv4:** 5.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-22859

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

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

131 **Оценка CVSSv4:** 5.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22853

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

132 **Оценка CVSSv4:** 6.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

133

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-22852

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FreeRDP: 3.0.0 - 3.20.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 6.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-9chc-g79v-4qq4https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47v9-p4gp-w5chhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-56f5-76qv-2r36https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmqf-m84q-x896https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4gxq-jhq6-4cr8https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w842-c386-fxhvhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rwp3-g84r-6mx9https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-47vj-g3c3-3rmfhttps://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8g87-6pvc-wh99

134

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24682

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

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

135

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24683

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

136

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24676

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 7.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

137

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24677

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

138

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24678

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

139

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24684

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

140

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24679

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

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

141

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24681

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

142

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24675

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 7.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

143

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24491

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 7.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

144

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-24680

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

145

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-23948

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: FreeRDP: 3.0.0 - 3.21.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

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: 6.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-10 / 2026-02-10

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6f3c-qvqq-2px5
- https://github.com/FreeRDP/FreeRDP/commit/4d44e3c097656a8b9ec696353647b0888ca45860
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j893-9wg8-33rc
- https://github.com/FreeRDP/FreeRDP/commit/c42ecbd183b001e76bfc3614cddfad0034acc758
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4x6j-w49r-869g
- https://github.com/FreeRDP/FreeRDP/commit/e02e052f6692550e539d10f99de9c35a23492db2
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x9jr-99h2-g7mj
- https://github.com/FreeRDP/FreeRDP/commit/d676518809c319eec15911c705c13536036af2ae
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ccvv-hg2w-6x9j
- https://github.com/FreeRDP/FreeRDP/commit/414f701464929c217f2509bcbd6d2c1f00f7ed73
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2jp4-67x6-gv7x
- https://github.com/FreeRDP/FreeRDP/commit/2d563a50be17c1b407ca448b1321378c0726dd31

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcgv-xgjp-h83q
- https://github.com/FreeRDP/FreeRDP/commit/622bb7b4402491ca003f47472d0e478132673696
- https://github.com/FreeRDP/FreeRDP/commit/afa6851dc80835d3101e40fcef51b6c5c0f43ea5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6gvg-29wx-6v7h
- https://github.com/FreeRDP/FreeRDP/commit/f3ab1a16139036179d9852745fdade18fec11600
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xw37-j744-f8v7
- https://github.com/FreeRDP/FreeRDP/commit/d2d4f449312ddafd4a4c6c8a4f856c7f0d44a3b5
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qh5p-frq4-pgxj
- https://github.com/FreeRDP/FreeRDP/commit/026b81ae5831ac1598d8f7371e0d0996fac7db00
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-45pf-68pj-fg8q
- https://github.com/FreeRDP/FreeRDP/commit/d9ca272dce7a776ab475e9b1a8e8c3d2968c8486
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vcw2-pqgw-mx6g
- https://github.com/FreeRDP/FreeRDP/commit/1c5c74223179d425a1ce6dbbb6a3dd2a958b7aee

146

Краткое описание: Обход безопасности в gogs

Идентификатор уязвимости: CVE-2025-64175

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: gogs: 0.13.0 - 0.13.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 7.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://github.com/gogs/gogs/security/advisories/GHSA-gg64-xxr9-qhjphttps://github.com/gogs/gogs/security/advisories/GHSA-mrph-w4hh-gx3ghttps://github.com/gogs/gogs/security/advisories/GHSA-5qhx-gwfj-6jqrhttps://github.com/gogs/gogs/security/advisories/GHSA-jp7c-wj6q-3qf2https://github.com/gogs/gogs/security/advisories/GHSA-cr88-6mqm-4g57https://github.com/gogs/gogs/security/advisories/GHSA-rjv5-9px2-fqw6https://github.com/gogs/gogs/security/advisories/GHSA-p6x6-9mx6-26wj

147

Краткое описание: Перезапись произвольных файлов в gogs

Идентификатор уязвимости: CVE-2026-24135

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

Уязвимый продукт: gogs: 0.13.0 - 0.13.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 7.0 AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://github.com/gogs/gogs/security/advisories/GHSA-gg64-xxr9-qhjp
- https://github.com/gogs/gogs/security/advisories/GHSA-mrph-w4hh-gx3g
- https://github.com/gogs/gogs/security/advisories/GHSA-5qhx-gwfj-6jqr
- https://github.com/gogs/gogs/security/advisories/GHSA-jp7c-wj6q-3qf2
- https://github.com/gogs/gogs/security/advisories/GHSA-cr88-6mqm-4g57
- https://github.com/gogs/gogs/security/advisories/GHSA-rjv5-9px2-fqw6
- https://github.com/gogs/gogs/security/advisories/GHSA-p6x6-9mx6-26wj

Краткое описание: Выполнение произвольного кода в gogs

Идентификатор уязвимости: CVE-2025-64111

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

Уязвимый продукт: gogs: 0.13.0 - 0.13.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: 9.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://github.com/gogs/gogs/security/advisories/GHSA-gg64-xxr9-qhjp
- https://github.com/gogs/gogs/security/advisories/GHSA-mrph-w4hh-gx3g
- https://github.com/gogs/gogs/security/advisories/GHSA-5qhx-gwfj-6jqr
- https://github.com/gogs/gogs/security/advisories/GHSA-jp7c-wj6q-3qf2
- https://github.com/gogs/gogs/security/advisories/GHSA-cr88-6mqm-4g57
- https://github.com/gogs/gogs/security/advisories/GHSA-rjv5-9px2-fqw6
- https://github.com/gogs/gogs/security/advisories/GHSA-p6x6-9mx6-26wj

149

Краткое описание: Получение конфиденциальной информации в JetBrains Hub

Идентификатор уязвимости: CVE-2026-25848

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: Hub: 2025.1.62455 - 2025.3.119033

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://www.jetbrains.com/privacy-security/issues-fixed/#ba7fe4fc4a7e651624a117e8bb8e30fe

150

Краткое описание: Запись локальных файлов в n8n

Идентификатор уязвимости: CVE-2026-25055

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

Уязвимый продукт: n8n: 1.123.0 - 2.2.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 7.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-06 / 2026-02-06

Ссылки на источник:

- https://github.com/n8n-io/n8n/security/advisories/GHSA-m82q-59gv-mcr9

151

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-1862

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 144.0.3719.104

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-06 / 2026-02-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-1861https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-1862

152

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-1861

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 144.0.3719.104

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-06 / 2026-02-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-1861https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-1862

153

Краткое описание: Выполнение произвольного кода в Autodesk Arnold

Идентификатор уязвимости: CVE-2026-0659

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Arnold components for USD: 7.4.0.0 - 7.4.4.1
Arnold: 7.4.0.0 - 7.4.4.1
Autodesk 3ds Max: 2026.1 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0003

154

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0662

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

155

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0660

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

156

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0536

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

157

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

158

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0661

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

159

Краткое описание: Выполнение произвольного кода в Autodesk 3ds Max

Идентификатор уязвимости: CVE-2026-0538

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk 3ds Max: 2026.0 - 2026.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-05 / 2026-02-05

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0002

160

Краткое описание: Получение конфиденциальной информации в GNU C Library (glibc)

Идентификатор уязвимости: CVE-2026-0915

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: GNU C Library (glibc): 2.0 - 2.42

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

Способ эксплуатации: Отправка пользователем запроса к вредоносному серверу

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: 2026-02-04 / 2026-02-04

Ссылки на источник:

- https://sourceware.org/bugzilla/show_bug.cgi?id=33814
- http://www.openwall.com/lists/oss-security/2026/01/20/3
- https://sourceware.org/bugzilla/show_bug.cgi?id=33796
- https://sourceware.org/git/?p=glibc.git;a=blob_plain;f=advisories/GLIBC-SA-2026-0001
- http://www.openwall.com/lists/oss-security/2026/01/16/5
- https://sourceware.org/bugzilla/show_bug.cgi?id=33802
- http://www.openwall.com/lists/oss-security/2026/01/16/6

161

Краткое описание: Выполнение произвольного кода в GNU C Library (glibc)

Идентификатор уязвимости: CVE-2026-0861

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

Уязвимый продукт: GNU C Library (glibc): 2.0 - 2.42

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

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-04 / 2026-02-04

Ссылки на источник:

- https://sourceware.org/bugzilla/show_bug.cgi?id=33814
- http://www.openwall.com/lists/oss-security/2026/01/20/3
- https://sourceware.org/bugzilla/show_bug.cgi?id=33796
- https://sourceware.org/git/?p=glibc.git;a=blob_plain;f=advisories/GLIBC-SA-2026-0001
- http://www.openwall.com/lists/oss-security/2026/01/16/5
- https://sourceware.org/bugzilla/show_bug.cgi?id=33802
- http://www.openwall.com/lists/oss-security/2026/01/16/6

162

Краткое описание: Отказ в обслуживании в GNU C Library (glibc)

Идентификатор уязвимости: CVE-2025-15281

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: GNU C Library (glibc): 2.0 - 2.42

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

Способ эксплуатации: Отправка специально сформированных 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: 2026-02-04 / 2026-02-04

Ссылки на источник:

- https://sourceware.org/bugzilla/show_bug.cgi?id=33814
- http://www.openwall.com/lists/oss-security/2026/01/20/3
- https://sourceware.org/bugzilla/show_bug.cgi?id=33796
- https://sourceware.org/git/?p=glibc.git;a=blob_plain;f=advisories/GLIBC-SA-2026-0001
- http://www.openwall.com/lists/oss-security/2026/01/16/5
- https://sourceware.org/bugzilla/show_bug.cgi?id=33802
- http://www.openwall.com/lists/oss-security/2026/01/16/6

163

Краткое описание: Выполнение произвольного кода в React Native Community CLI

Идентификатор уязвимости: CVE-2025-11953

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

Уязвимый продукт: React Native Community CLI: 17.0.0 - 19.1.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных 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: 2026-02-03 / 2026-02-03

Ссылки на источник:

- https://github.com/advisories/GHSA-399j-vxmf-hjvr
- https://github.com/react-native-community/cli/commit/15089907d1f1301b22c72d7f68846a2ef20df547

164

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2026-1285

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Django: 4.0 - 6.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-02-03 / 2026-02-03

Ссылки на источник:

- https://www.djangoproject.com/weblog/2026/feb/03/security-releases/

165

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2025-14550

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Django: 4.0 - 6.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-02-03 / 2026-02-03

Ссылки на источник:

- https://www.djangoproject.com/weblog/2026/feb/03/security-releases/

166

Краткое описание: Обход безопасности в WatchGuard Firebox Fireware OS

Идентификатор уязвимости: CVE-2026-1498

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: Fireware OS: 12.0 - 2025.1.4

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Некорректная проверка входных данных.

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: Не определено

Оценка CVSSv4: 7.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2026-01-30 / 2026-01-30

Ссылки на источник:

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00001

167

Краткое описание: Выполнение произвольного кода в QNAP QTS

Идентификатор уязвимости: CVE-2025-66276

Идентификатор программной ошибки: Не определено

Уязвимый продукт: QNAP QTS: 4.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 8.1 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: 2026-01-30 / 2026-01-30

Ссылки на источник:

- https://www.qnap.com/en/security-advisory/qsa-25-56

168

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-22258
BDU:2026-00955

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

Уязвимый продукт: Suricata: 7.0.0 - 8.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-01-28 / 2026-01-28

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-878h-2x6v-84q9
- https://github.com/OISF/suricata/security/advisories/GHSA-5jvg-5j3p-34cf
- https://github.com/OISF/suricata/security/advisories/GHSA-9qg5-2gwh-xp86
- https://github.com/OISF/suricata/security/advisories/GHSA-rwc5-hxj6-hwx7
- https://github.com/OISF/suricata/security/advisories/GHSA-mqr8-m3m4-2hw5
- https://github.com/OISF/suricata/security/advisories/GHSA-3gm8-84cm-5x22
- https://github.com/OISF/suricata/security/advisories/GHSA-289c-h599-3xcx
- https://bdu.fstec.ru/vul/2026-00955

169

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-22260
BDU:2026-00952

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Suricata: 7.0.0 - 8.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-01-28 / 2026-01-28

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-878h-2x6v-84q9https://github.com/OISF/suricata/security/advisories/GHSA-5jvg-5j3p-34cfhttps://github.com/OISF/suricata/security/advisories/GHSA-9qg5-2gwh-xp86https://github.com/OISF/suricata/security/advisories/GHSA-rwc5-hxj6-hwx7https://github.com/OISF/suricata/security/advisories/GHSA-mqr8-m3m4-2hw5https://github.com/OISF/suricata/security/advisories/GHSA-3gm8-84cm-5x22https://github.com/OISF/suricata/security/advisories/GHSA-289c-h599-3xcx
- https://bdu.fstec.ru/vul/2026-00952

170

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-22259
BDU:2026-00953

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

Уязвимый продукт: Suricata: 7.0.0 - 8.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-01-28 / 2026-01-28

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-878h-2x6v-84q9
- https://github.com/OISF/suricata/security/advisories/GHSA-5jvg-5j3p-34cf
- https://github.com/OISF/suricata/security/advisories/GHSA-9qg5-2gwh-xp86
- https://github.com/OISF/suricata/security/advisories/GHSA-rwc5-hxj6-hwx7
- https://github.com/OISF/suricata/security/advisories/GHSA-mqr8-m3m4-2hw5
- https://github.com/OISF/suricata/security/advisories/GHSA-3gm8-84cm-5x22
- https://github.com/OISF/suricata/security/advisories/GHSA-289c-h599-3xcx
- https://bdu.fstec.ru/vul/2026-00953

171

Краткое описание: Отказ в обслуживании в OpenSSL

Идентификатор уязвимости: CVE-2025-69421
BDU:2026-01218

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: OpenSSL: 1.0.2 - 3.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 2026-01-27 / 2026-02-06

Ссылки на источник:

- https://openssl-library.org/news/secadv/20260127.txt
- https://bdu.fstec.ru/vul/2026-01218

172

Краткое описание: Отказ в обслуживании в OpenSSL

Идентификатор уязвимости: CVE-2025-69420
BDU:2026-01219

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

Уязвимый продукт: OpenSSL: 1.0.2 - 3.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-01-27 / 2026-02-06

Ссылки на источник:

- https://openssl-library.org/news/secadv/20260127.txt
- https://bdu.fstec.ru/vul/2026-01219

173

Краткое описание: Выполнение произвольного кода в OpenSSL

Идентификатор уязвимости: CVE-2025-15467
BDU:2026-00890

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: OpenSSL: 1.0.2 - 3.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных 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: 2026-01-27 / 2026-02-06

Ссылки на источник:

- https://openssl-library.org/news/secadv/20260127.txt
- https://bdu.fstec.ru/vul/2026-00890

174

Краткое описание: Выполнение произвольного кода в xrdp

Идентификатор уязвимости: CVE-2025-68670
BDU:2026-00962

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: xrdp: 0.10.0 - 0.10.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-28 / 2026-01-28

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-rwvg-gp87-gh6f
- https://bdu.fstec.ru/vul/2026-00962

175

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-24869
BDU:2026-00970

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 147.0 - 147.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-27 / 2026-01-27

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-06/https://bugzilla.mozilla.org/show_bug.cgi?id=2007302https://bugzilla.mozilla.org/show_bug.cgi?id=2008698
- https://bdu.fstec.ru/vul/2026-00970