НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-08-19.1 | 19 августа 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-55134	Microsoft Word	Локальный	ACE	2026-07-29	✓
2	Высокая	CVE-2026-8512	Google Chrome	Сетевой	ACE	2026-07-30	✓
3	Высокая	CVE-2026-8514	Google Chrome	Сетевой	ACE	2026-07-30	✓
4	Высокая	CVE-2026-8515	Google Chrome	Сетевой	ACE	2026-07-30	✓
5	Высокая	CVE-2026-8517	Google Chrome	Сетевой	DoS	2026-07-30	✓
6	Высокая	CVE-2026-55127	Microsoft Word	Локальный	ACE	2026-07-30	✓
7	Высокая	CVE-2026-8520	Google Chrome	Сетевой	DoS	2026-07-31	✓
8	Высокая	CVE-2026-8521	Google Chrome	Смежная сеть	ACE	2026-07-31	✓
9	Критическая	CVE-2026-8511	Google Chrome	Сетевой	ACE	2026-07-30	✓
10	Высокая	CVE-2026-8518	Google Chrome	Сетевой	ACE	2026-07-31	✓
11	Высокая	CVE-2026-8509	Google Chrome	Сетевой	ACE	2026-07-30	✓
12	Критическая	CVE-2026-51291	SQLite	Сетевой	ACE	2026-07-31	✓
13	Высокая	CVE-2026-55125	Microsoft Office	Локальный	ACE	2026-07-30	✓

14	Критическая	CVE-2026-51290	SQLite	Сетевой	DoS	2026-07-31	✓
15	Высокая	CVE-2026-6267	Gitlab	Сетевой	ACE	2026-07-16	✓
16	Высокая	CVE-2026-12436	Gitlab	Сетевой	Не определено	2026-07-16	✓
17	Высокая	CVE-2026-42900	Microsoft Windows App Store	Сетевой	PE	2026-07-30	✓
18	Высокая	CVE-2026-8522	Google Chrome	Сетевой	ACE	2026-07-31	✓
19	Критическая	CVE-2026-6919	Google Chrome	Сетевой	ACE	2026-07-30	✓
20	Высокая	CVE-2026-55036	Office Online Server	Локальный	ACE	2026-07-30	✓
21	Высокая	CVE-2026-8523	Google Chrome	Сетевой	ACE	2026-07-31	✓
22	Высокая	CVE-2026-8525	Google Chrome	Сетевой	ACE	2026-07-31	✓
23	Высокая	BDU:2026-10853	РЕД ОС	Сетевой	ACE	2026-07-28	✓
24	Высокая	CVE-2026-55038	Microsoft Word	Локальный	ACE	2026-07-29	✓
25	Высокая	CVE-2026-34480	Apache Log4j Core	Сетевой	LoI	2026-07-23	✓
26	Критическая	CVE-2026-41635	Apache MINA	Сетевой	ACE	2026-07-23	✓
27	Высокая	CVE-2026-33750	brace-expansion	Сетевой	DoS	2026-07-23	✓
28	Высокая	CVE-2026-27830	c3p0	Смежная сеть	ACE	2026-07-23	✓

29	Высокая	CVE-2026-55045	Microsoft Office	Локальный	ACE	2026-07-29	✓
30	Критическая	CVE-2026-40477	Thymeleaf	Сетевой	SB	2026-07-23	✓
31	Высокая	CVE-2026-31768	Linux	Локальный	ACE	2026-07-23	✓
32	Высокая	CVE-2026-31758	Linux	Локальный	ACE	2026-07-23	✓
33	Высокая	CVE-2026-31720	Linux	Локальный	ACE	2026-07-23	✓
34	Высокая	CVE-2026-31743	Linux	Локальный	ACE	2026-07-23	✓
35	Высокая	CVE-2026-31700	Linux	Локальный	ACE	2026-07-23	✓
36	Высокая	CVE-2026-31690	Linux	Локальный	ACE	2026-07-23	✓
37	Высокая	CVE-2026-31742	Linux	Локальный	ACE	2026-07-23	✓
38	Высокая	CVE-2026-23458	Linux	Локальный	ACE	2026-07-23	✓
39	Высокая	CVE-2026-23288	Linux	Локальный	ACE	2026-07-23	✓
40	Высокая	CVE-2026-23451	Linux	Сетевой	DoS	2026-07-23	✓
41	Высокая	CVE-2026-31787	Linux	Локальный	ACE	2026-07-23	✓
42	Высокая	CVE-2026-31782	Linux	Локальный	ACE	2026-07-23	✓
43	Высокая	CVE-2026-8524	Google Chrome	Сетевой	ACE	2026-07-31	✓

44	Высокая	CVE-2026-41907	uuid	Сетевой	ACE	2026-07-23	✓
45	Высокая	CVE-2026-7379	Wireshark	Сетевой	DoS	2026-05-05	✓
46	Высокая	CVE-2026-7376	Wireshark	Сетевой	DoS	2026-05-05	✓
47	Высокая	CVE-2026-8526	Google Chrome	Сетевой	ACE	2026-07-31	✓
48	Высокая	CVE-2026-8527	Google Chrome	Сетевой	DoS	2026-07-31	✓
49	Высокая	CVE-2026-42129	Grafana	Сетевой	OSI	2026-07-28	✓
50	Высокая	CVE-2026-42127	Grafana	Сетевой	DoS	2026-07-28	✓
51	Высокая	CVE-2026-47162	vim	Сетевой	ACE	2026-07-30	✓
52	Высокая	CVE-2026-42198	JDBC pgjdbc	Сетевой	DoS	2026-07-28	✓
53	Высокая	CVE-2026-7378	Wireshark	Сетевой	DoS	2026-05-05	✓
54	Высокая	CVE-2026-44307	mako	Сетевой	OSI	2026-07-29	✓
55	Высокая	CVE-2026-41292	Unbound	Сетевой	DoS	2026-07-28	✓
56	Высокая	CVE-2026-42311	Pillow	Локальный	DoS	2026-07-29	✓
57	Высокая	CVE-2026-41205	mako	Сетевой	OSI	2026-07-28	✓
58	Высокая	CVE-2026-52726	python-dulwich	Сетевой	OSI	2026-07-29	✓

59	Критическая	CVE-2026-55040	Microsoft SharePoint Server	Сетевой	SB	2026-07-29	✓
60	Высокая	CVE-2026-7375	Wireshark	Сетевой	DoS	2026-05-05	✓
61	Высокая	CVE-2026-6868	Wireshark	Сетевой	DoS	2026-05-05	✓
62	Высокая	CVE-2026-56370	ImageMagick	Локальный	ACE	2026-07-16	✓
63	Высокая	CVE-2026-55034	Microsoft SharePoint Server	Сетевой	SB	2026-07-29	✓
64	Высокая	CVE-2026-28737	Gitea	Сетевой	XSS\CSS	2026-07-28	✓
65	Высокая	CVE-2026-28699	Gitea	Сетевой	PE	2026-07-28	✓
66	Высокая	CVE-2026-44244	GitPython	Локальный	ACE	2026-07-29	✓
67	Критическая	CVE-2026-44243	GitPython	Сетевой	OSI	2026-07-29	✓
68	Критическая	CVE-2026-42563	python-dulwich	Сетевой	ACE	2026-07-29	✓
69	Высокая	CVE-2026-42046	libcaca	Локальный	ACE	2026-07-28	✓
70	Критическая	CVE-2026-47304	.NET	Сетевой	SB	2026-07-30	✓
71	Высокая	CVE-2026-55128	Microsoft Word	Локальный	ACE	2026-06-10	✓
72	Высокая	CVE-2026-55032	Microsoft Word	Локальный	ACE	2026-06-10	✓
73	Высокая	CVE-2026-8389	Firefox	Сетевой	ACE	2026-08-03	✓

74	Высокая	CVE-2026-55132	Microsoft Word	Локальный	ACE	2026-05-14	✓
75	Высокая	CVE-2026-47302	.NET	Сетевой	DoS	2026-07-29	✓
76	Высокая	CVE-2026-9277	shell-quote	Сетевой	ACE	2026-08-03	✓
77	Высокая	CVE-2026-47295	Microsoft SQL Server	Сетевой	PE	2026-07-30	✓
78	Высокая	CVE-2026-50387	Windows GDI	Локальный	PE	2026-07-30	✓
79	Высокая	CVE-2026-50368	Windows Active Directory Federation Services	Сетевой	DoS	2026-07-24	✓
80	Критическая	CVE-2026-44262	Scramble	Сетевой	ACE	2026-08-03	✓
81	Критическая	CVE-2026-47668	DbGate	Сетевой	ACE	2026-08-03	✓
82	Высокая	CVE-2026-50653	Azure Active Directory	Сетевой	DoS	2026-07-30	✓
83	Высокая	CVE-2026-58527	Windows Runtime	Локальный	PE	2026-07-16	✓
84	Высокая	CVE-2026-8390	Firefox	Сетевой	ACE	2026-08-03	✓
85	Высокая	CVE-2026-50650	.NET	Локальный	PE	2026-07-29	✓
86	Высокая	CVE-2026-8529	Google Chrome	Сетевой	ACE	2026-07-31	✓
87	Высокая	CVE-2026-8532	Google Chrome	Сетевой	ACE	2026-07-31	✓
88	Высокая	CVE-2026-8533	Google Chrome	Сетевой	ACE	2026-07-31	✓

89	Высокая	CVE-2026-8534	Google Chrome	Сетевой	ACE	2026-07-31	✓
90	Высокая	CVE-2026-8544	Google Chrome	Сетевой	ACE	2026-07-31	✓
91	Высокая	CVE-2026-8548	Google Chrome	Сетевой	ACE	2026-07-31	✓
92	Высокая	CVE-2026-8540	Google Chrome	Сетевой	ACE	2026-07-31	✓
93	Высокая	CVE-2026-8551	Google Chrome	Сетевой	ACE	2026-07-31	✓
94	Высокая	CVE-2026-8557	Google Chrome	Сетевой	ACE	2026-07-31	✓
95	Высокая	CVE-2026-8558	Google Chrome	Сетевой	ACE	2026-07-31	✓
96	Высокая	CVE-2026-8575	Google Chrome	Сетевой	ACE	2026-07-31	✓
97	Высокая	CVE-2026-68580	FreeRDP	Сетевой	DoS	2026-08-03	✓
98	Высокая	CVE-2026-8569	Google Chrome	Сетевой	ACE	2026-07-31	✓
99	Высокая	CVE-2026-50525	.NET	Сетевой	DoS	2026-07-29	✓
100	Высокая	CVE-2026-8549	Google Chrome	Сетевой	ACE	2026-07-31	✓
101	Высокая	CVE-2026-55255	Langflow	Сетевой	SB	2026-08-04	✓
102	Высокая	CVE-2026-67304	FreeRDP	Сетевой	DoS	2026-08-04	✓
103	Критическая	CVE-2026-53412	Zoom Meeting SDK for Windows	Сетевой	ACE	2026-07-16	✓

104	Высокая	CVE-2026-67298	FreeRDP	Сетевой	DoS	2026-08-04	✓
105	Высокая	CVE-2026-67297	FreeRDP	Сетевой	DoS	2026-08-04	✓
106	Высокая	CVE-2026-67296	FreeRDP	Сетевой	DoS	2026-08-04	✓
107	Высокая	CVE-2026-67291	FreeRDP	Сетевой	DoS	2026-08-04	✓
108	Высокая	CVE-2026-67290	FreeRDP	Сетевой	DoS	2026-08-04	✓
109	Критическая	CVE-2026-67289	FreeRDP	Сетевой	ACE	2026-08-04	✓
110	Высокая	CVE-2026-67299	FreeRDP	Сетевой	ACE	2026-08-04	✓
111	Высокая	CVE-2026-9998	Google Chrome	Сетевой	DoS	2026-08-03	✓
112	Высокая	CVE-2026-10001	Google Chrome	Сетевой	DoS	2026-08-02	✓
113	Высокая	CVE-2026-10002	Google Chrome	Сетевой	DoS	2026-08-02	✓
114	Высокая	CVE-2026-10003	Google Chrome	Сетевой	DoS	2026-08-02	✓
115	Высокая	CVE-2026-10006	Google Chrome	Сетевой	DoS	2026-08-02	✓
116	Высокая	CVE-2026-10007	Google Chrome	Сетевой	DoS	2026-08-02	✓
117	Высокая	CVE-2026-10009	Google Chrome	Сетевой	DoS	2026-08-02	✓
118	Высокая	CVE-2026-10013	Google Chrome	Сетевой	DoS	2026-08-02	✓

119	Высокая	CVE-2026-10012	Google Chrome	Сетевой	DoS	2026-08-02	✓
120	Высокая	CVE-2026-10015	Google Chrome	Сетевой	DoS	2026-08-02	✓
121	Высокая	CVE-2026-10016	Google Chrome	Сетевой	DoS	2026-08-02	✓
122	Высокая	CVE-2026-10017	Google Chrome	Сетевой	DoS	2026-08-02	✓
123	Высокая	CVE-2026-10019	Google Chrome	Сетевой	DoS	2026-08-02	✓
124	Высокая	CVE-2026-10021	Google Chrome	Сетевой	DoS	2026-08-02	✓
125	Высокая	CVE-2026-34092	MediaWiki	Сетевой	OSI	2026-08-04	✓
126	Высокая	CVE-2026-34091	MediaWiki	Сетевой	OSI	2026-08-04	✓
127	Высокая	CVE-2026-34088	MediaWiki	Сетевой	OSI	2026-08-04	✓
128	Высокая	CVE-2026-67322	GitPython	Сетевой	OSI	2026-08-05	✓
129	Высокая	CVE-2026-67323	GitPython	Локальный	ACE	2026-08-05	✓
130	Критическая	CVE-2026-67324	GitPython	Сетевой	ACE	2026-08-05	✓
131	Высокая	CVE-2026-67325	GitPython	Сетевой	ACE	2026-08-05	✓
132	Критическая	CVE-2026-69240	Sequelize	Сетевой	ACE	2026-08-05	✓
133	Высокая	CVE-2026-69249	cryptography	Сетевой	DoS	2026-08-05	✓

134	Высокая	CVE-2026-32775	Libexif	Локальный	DoS	2026-07-31	✓
135	Критическая	CVE-2026-33278	Unbound	Сетевой	DoS	2026-07-31	✓
136	Критическая	CVE-2026-33322	MinIO	Сетевой	PE	2026-07-31	✓
137	Высокая	CVE-2026-33419	MinIO	Сетевой	OSI	2026-07-31	✓
138	Высокая	CVE-2026-33641	Glances	Локальный	PE	2026-07-31	✓
139	Высокая	CVE-2026-34087	MediaWiki	Сетевой	OSI	2026-08-04	✓
140	Высокая	CVE-2026-10022	Google Chrome	Сетевой	DoS	2026-08-02	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55134
BDU:2026-10687

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5561.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55134
- https://bdu.fstec.ru/vul/2026-10687

2

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8512
BDU:2026-10784

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-8747-7f43-99gq
- https://issues.Google Chrome.org/issues/495782021
- https://nvd.nist.gov/vuln/detail/CVE-2026-8512
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8512
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8512
- https://security-tracker.debian.org/tracker/CVE-2026-8512

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10784

3

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8514
BDU:2026-10785

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-cg64-j5p6-4xrq
- https://issues.Google Chrome.org/issues/495948109
- https://nvd.nist.gov/vuln/detail/CVE-2026-8514
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8514
- https://security-tracker.debian.org/tracker/CVE-2026-8514
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8514

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10785

4

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8515
BDU:2026-10786

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-57r7-2v6h-4x36
- https://issues.Google Chrome.org/issues/495999127
- https://nvd.nist.gov/vuln/detail/CVE-2026-8515
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8515
- https://security-tracker.debian.org/tracker/CVE-2026-8515
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF

- https://bdu.fstec.ru/vul/2026-10786

5

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8517
BDU:2026-10788

Идентификатор программной ошибки: CWE-664 Некорректное обращение с ресурсом на протяжении его жизненного цикла

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-x28c-6463-7xg5
- https://issues.Google Chrome.org/issues/497531263
- https://nvd.nist.gov/vuln/detail/CVE-2026-8517
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8517
- https://security-tracker.debian.org/tracker/CVE-2026-8517
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8517
- https://bdu.fstec.ru/vul/2026-10788

6

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55127
BDU:2026-10739

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55127
- https://bdu.fstec.ru/vul/2026-10739

7

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8520
BDU:2026-10790

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-jg93-pv2v-839r
- https://issues.Google Chrome.org/issues/503619813
- https://nvd.nist.gov/vuln/detail/CVE-2026-8520
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8520
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8520

- https://security-tracker.debian.org/tracker/CVE-2026-8520
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10790

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8521
BDU:2026-10791

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-9mx2-vh7f-423c
- https://issues.Google Chrome.org/issues/504106200
- https://nvd.nist.gov/vuln/detail/CVE-2026-8521
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8521
- https://security-tracker.debian.org/tracker/CVE-2026-8521
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8521

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10791

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8511
BDU:2026-10783

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-5w85-m7vr-r7mx
- https://issues.Google Chrome.org/issues/495108488
- https://nvd.nist.gov/vuln/detail/CVE-2026-8511
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8511
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8511
- https://security-tracker.debian.org/tracker/CVE-2026-8511

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10783

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8518
BDU:2026-10789

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-3p4x-fwpx-xpr8
- https://issues.Google Chrome.org/issues/497830330
- https://nvd.nist.gov/vuln/detail/CVE-2026-8518
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8518
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8518
- https://security-tracker.debian.org/tracker/CVE-2026-8518

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10789

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8509
BDU:2026-10782

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-87wp-w4rq-jfvp
- https://issues.Google Chrome.org/issues/493310462
- https://nvd.nist.gov/vuln/detail/CVE-2026-8509
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8509
- https://security-tracker.debian.org/tracker/CVE-2026-8509
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8509

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10782

12

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51291
BDU:2026-10774

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: до 3.41.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51291
- https://github.com/sqlite/sqlite/blob/master/src/json.c
- https://bdu.fstec.ru/vul/2026-10774

13

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-55125
BDU:2026-10776

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55125
- https://bdu.fstec.ru/vul/2026-10776

14

Краткое описание: Отказ в обслуживании в SQLite

Идентификатор уязвимости: CVE-2026-51290
BDU:2026-10773

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: SQLite: 3.41

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51290md
- https://github.com/sqlite/sqlite/blob/master/src/btree.c
- https://bdu.fstec.ru/vul/2026-10773

15

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-6267
BDU:2026-10766

Идентификатор программной ошибки: CWE-201 Включение важной информации в отправляемые данные

Уязвимый продукт: Gitlab: от 10.1.0 до 19.0.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-1-released/
- https://hackerone.com/reports/3658324
- https://bdu.fstec.ru/vul/2026-10766

16

Краткое описание: Уязвимость в Gitlab

Идентификатор уязвимости: CVE-2026-12436
BDU:2026-10765

Идентификатор программной ошибки: CWE-915 Некорректный контроль над изменением динамически определяемых атрибутов объектов

Уязвимый продукт: Gitlab: от 19.2 до 19.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Не определено

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-1-released/
- https://hackerone.com/reports/3800511
- https://bdu.fstec.ru/vul/2026-10765

17

Краткое описание: Повышение привилегий в Microsoft Windows App Store

Идентификатор уязвимости: CVE-2026-42900
BDU:2026-10763

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: 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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42900
- https://bdu.fstec.ru/vul/2026-10763

18

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8522
BDU:2026-10793

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-j89q-h74w-5c2q
- https://issues.Google Chrome.org/issues/504185107
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8522
- https://security-tracker.debian.org/tracker/CVE-2026-8522
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8522
- https://bdu.fstec.ru/vul/2026-10793

19

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-6919
BDU:2026-10781

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 147.0.7727.116
Microsoft Edge: до 147.0.3912.87
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_22.html
- https://github.com/advisories/GHSA-cxc8-7952-8cj3
- https://issues.Google Chrome.org/issues/493652473
- https://nvd.nist.gov/vuln/detail/CVE-2026-6919
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-6919
- https://security-tracker.debian.org/tracker/CVE-2026-6919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-6919

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10781

20

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-55036
BDU:2026-10760

Идентификатор программной ошибки: CWE-126 Чтение за границей буфера

Уязвимый продукт: Office Online Server: до 16.0.10417.20175
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Excel 2016: до 16.0.5561.1001
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55036
- https://bdu.fstec.ru/vul/2026-10760

21

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8523
BDU:2026-10794

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-937x-29v2-25x3
- https://issues.Google Chrome.org/issues/483956252
- https://nvd.nist.gov/vuln/detail/CVE-2026-8523
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8523
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8523
- https://security-tracker.debian.org/tracker/CVE-2026-8523

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10794

22

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8525
BDU:2026-10796

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-ghgw-c29j-38q7
- https://issues.Google Chrome.org/issues/497928952
- https://nvd.nist.gov/vuln/detail/CVE-2026-8525
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8525
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8525
- https://security-tracker.debian.org/tracker/CVE-2026-8525
- https://bdu.fstec.ru/vul/2026-10796

23

Краткое описание: Выполнение произвольного кода в РЕД ОС

Идентификатор уязвимости: BDU:2026-10853

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

Уязвимый продукт: РЕД ОС: 8.0

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

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-10853

24

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55038
BDU:2026-10855

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5561.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55038
- https://bdu.fstec.ru/vul/2026-10855

25

Краткое описание: Потеря целостности в Apache Log4j Core

Идентификатор уязвимости: CVE-2026-34480
BDU:2026-10856

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

Уязвимый продукт: Apache Log4j Core: от 3.0.0-alpha1 до 3.0.0-beta3 включительно
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Потеря целостности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://github.com/apache/logging-log4j2/pull/4077
- https://logging.apache.org/security.html#CVE-2026-34480
- https://lists.apache.org/thread/5x0hcnng0chhghp6jgjdp3qmbbhfjzhb
- https://bdu.fstec.ru/vul/2026-10856

26

Краткое описание: Выполнение произвольного кода в Apache MINA

Идентификатор уязвимости: CVE-2026-41635
BDU:2026-10859

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: MINA: от 2.0.0 до 2.0.27 включительно
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://lists.apache.org/thread/1l91w1mqsb3lwfd504fs045ylxntt2tm
- https://www.openwall.com/lists/oss-security/2026/04/27/4
- https://bdu.fstec.ru/vul/2026-10859

Краткое описание: Отказ в обслуживании в brace-expansion

Идентификатор уязвимости: CVE-2026-33750
BDU:2026-10879

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

Уязвимый продукт: brace-expansion: до 1.1.13
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

27

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

Ссылки на источник:

- http://github.com/juliangruber/brace-expansion/security/advisories/GHSA-f886-m6hf-6m8v
- https://github.com/juliangruber/brace-expansion/pull/97
- https://github.com/juliangruber/brace-expansion/pull/96
- https://github.com/juliangruber/brace-expansion/pull/95
- https://github.com/juliangruber/brace-expansion/issues/98
- https://github.com/juliangruber/brace-expansion/commit/b9cacd9e55e7a1fa588fe4b7bb1159d52f1d902a
- https://github.com/juliangruber/brace-expansion/commit/7fd684f89fdde3549563d0a6522226a9189472a2
- https://github.com/juliangruber/brace-expansion/commit/311ac0d54994158c0a384e286a7d6cbb17ee8ed5

- https://github.com/juliangruber/brace-expansion/blob/daa71bcb4a30a2df9bcb7f7b8daaf2ab30e5794a/src/index.ts#L184https://github.com/juliangruber/brace-expansion/blob/daa71bcb4a30a2df9bcb7f7b8daaf2ab30e5794a/src/index.ts#L107-L113
- https://bdu.fstec.ru/vul/2026-10879

28

Краткое описание: Выполнение произвольного кода в c3p0

Идентификатор уязвимости: CVE-2026-27830
BDU:2026-10880

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: c3p0: до 0.12.0
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://www.sentinelone.com/vulnerability-database/cve-2026-27830/
- https://github.com/swaldman/c3p0/commit/e14cbd8166e423e2e9a9d6f08b2add3433492d6e
- https://github.com/swaldman/c3p0/security/advisories/GHSA-5476-xc4j-rqcv
- https://www.mchange.com/projects/c3p0/#security-note
- https://bdu.fstec.ru/vul/2026-10880

29

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-55045
BDU:2026-10851

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55045
- https://bdu.fstec.ru/vul/2026-10851

Краткое описание: Обход безопасности в Thymeleaf

Идентификатор уязвимости: CVE-2026-40477
BDU:2026-10883

Идентификатор программной ошибки: CWE-1039 Некорректная работа автоматизированного механизма распознавания при определении или обработке входных данных, модифицированных злоумышленником

Уязвимый продукт: Thymeleaf: до 3.1.4.RELEASE
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

30 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://github.com/thymeleaf/thymeleaf/security/advisories/GHSA-r4v4-5mwr-2fwr
- https://bdu.fstec.ru/vul/2026-10883

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31768
BDU:2026-10887

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

Уязвимый продукт: Linux: от 4.9 до 6.1.167 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

31

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31768
- https://git.kernel.org/stable/c/b3bb8faeca1a2ef7be95ee8a512b639f9ffce947
- https://git.kernel.org/stable/c/fa64aab25aba47296aa8d12bb4c88ec3fecb2054
- https://git.kernel.org/stable/c/67b3a91bdc48220bfb67155ab528121b9c822782
- https://git.kernel.org/stable/c/014c6d27878d3883f7bb065610768fd021de1a96
- https://git.kernel.org/stable/c/d2d031b0786ea66ab0577c9d2d71435068d32199
- https://git.kernel.org/stable/c/768461517a28d80fe81ea4d5d03a90cd184ea6ad
- https://lore.kernel.org/linux-cve-announce/2026050147-CVE-2026-31768-6fbc@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31768

- https://bdu.fstec.ru/vul/2026-10887

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31758
BDU:2026-10888

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.19 до 5.10.252 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

32

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31758
- https://git.kernel.org/stable/c/959ef329071136e4335b54822fe2f607659b4569
- https://git.kernel.org/stable/c/e189d443767f7cd390c52f2e122e1fc41c7562d6
- https://git.kernel.org/stable/c/7fa8f61bab3fb75b5deba8a0f3abb74dc5068d9f
- https://git.kernel.org/stable/c/95e09b07e50290254b28b8395509473104518f8c
- https://git.kernel.org/stable/c/d13318dec0c1e0e2ac16f8ecbd522db14cea4bb1
- https://git.kernel.org/stable/c/977b632db51d231dec0bc571089a5c2402674139
- https://git.kernel.org/stable/c/d40198de50232e04c14c6e2092e896766c95ea48
- https://git.kernel.org/stable/c/8a768552f7a8276fb9e01d49773d2094ace7c8f1

- https://lore.kernel.org/linux-cve-announce/2026050144-CVE-2026-31758-8487@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31758
- https://access.redhat.com/security/cve/cve-2026-31758
- https://bdu.fstec.ru/vul/2026-10888

33

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31720
BDU:2026-10889

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.31 до 5.10.252 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://git.kernel.org/stable/c/c6da4fed7537aec19880c24f6c3a95065adb1406
- https://git.kernel.org/stable/c/21b11e8581285c6f10ef43d05df349d445f24273
- https://git.kernel.org/stable/c/be2d32f0c3fe333d14c0a9ca90328dacbc3e06b8
- https://git.kernel.org/stable/c/557d1d4e862eccd0b74cc377b66de3e1e8d49605
- https://git.kernel.org/stable/c/6e0e34d85cd46ceb37d16054e97a373a32770f6c
- https://git.kernel.org/stable/c/26304d124e7f0383f8fe1168b5801a0ac7e16b1c
- https://git.kernel.org/stable/c/0d41772d98dcaf6c17e875b7d0ea0154ae1191ee
- https://git.kernel.org/stable/c/8e5eb1d6e6a3d7bbea9c92132d0cda5793176426
- https://www.cve.org/CVERecord?id=CVE-2026-31720
- https://lore.kernel.org/linux-cve-announce/2026050131-CVE-2026-31720-3b60@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-31720
- https://bdu.fstec.ru/vul/2026-10889

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31743
BDU:2026-10890

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 6.9 до 6.12.80 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

34

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31743
- https://git.kernel.org/stable/c/2f6e5b9964d0a63a5ba84fca2642876afb70a662
- https://git.kernel.org/stable/c/784ed4abded1ca4b525fa4cade8b02f8c5d2a087
- https://git.kernel.org/stable/c/6c01e7f11f5e5f22285d19510a9643e2506e13c3
- https://git.kernel.org/stable/c/f9b88613ff402aa6fe8fd020573cb95867ae947e
- https://lore.kernel.org/linux-cve-announce/2026050140-CVE-2026-31743-e8c6@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31743
- https://bdu.fstec.ru/vul/2026-10890

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31700
BDU:2026-10891

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

Уязвимый продукт: Linux: от 4.6 до 6.6.135 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

35

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

Ссылки на источник:

- https://bdu.fstec.ru/vul/2026-10891
- https://git.kernel.org/stable/c/2c054e17d9d41f1020376806c7f750834ced4dc5
- https://git.kernel.org/stable/c/48a6ef291a17639e1b6ae0fbe9c8b2bb87d7804b
- https://git.kernel.org/stable/c/74e2db36fe50e3ad9d5300d7fd0e6e2a15a6d121
- https://git.kernel.org/stable/c/28324a3b62d9ce7f9bdd65a8ce63f382041d1b27
- https://git.kernel.org/stable/c/3a1bf9116ea31470b89692585c3910dfe830dcdd
- https://www.cve.org/CVERecord?id=CVE-2026-31700
- https://lore.kernel.org/linux-cve-announce/2026050119-CVE-2026-31700-c820@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31700

- Для продуктов Red Hat Inc.:
- https://access.redhat.com/security/cve/cve-2026-31700

36

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31690
BDU:2026-10892

Идентификатор программной ошибки: CWE-823 Использование для указателя смещения за пределами назначенного диапазона

Уязвимый продукт: Linux: от 6.15 до 6.18.22 включительно

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://git.kernel.org/stable/c/fbdb43f6bb2a15ed382d6eb0ef82c8b07b0d47bb
- https://git.kernel.org/stable/c/bd15a5deb5a7251dc1a0cf9186f0253f7eacdb97
- https://www.cve.org/CVERecord?id=CVE-2026-31690
- https://git.kernel.org/linus/88c4bd90725557796c15878b7cb70066e9e6b5ab
- https://lore.kernel.org/linux-cve-announce/2026042757-CVE-2026-31690-018e@gregkh/
- https://bdu.fstec.ru/vul/2026-10892

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31742
BDU:2026-10894

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 6.19.10 до 6.19.11 включительно
Red Hat Enterprise Linux: 10

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

37

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31742
- https://git.kernel.org/stable/c/891d790fdb5c96c6e1d2841e06ee6c360f2d1288
- https://git.kernel.org/stable/c/428fdf55301e6c8fa5a36b426240797b1cf86570
- https://git.kernel.org/stable/c/40014493cece72a0be5672cd86763e53fb3ec613
- https://lore.kernel.org/linux-cve-announce/2026050140-CVE-2026-31742-e1b4@gregkh/
- https://access.redhat.com/security/cve/cve-2026-31742
- https://bdu.fstec.ru/vul/2026-10894

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23458
BDU:2026-10895

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

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

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

38

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23458
- https://git.kernel.org/stable/c/bdf2724eefd4455a66863abb025bab8d3aa98c57
- https://git.kernel.org/stable/c/f04cc86d59906513d2d62183b882966fc0ae0390
- https://git.kernel.org/stable/c/f025171feef2ac65663d7986f1d5ff0c28d6b2a9
- https://git.kernel.org/stable/c/04c8907ce4e3d3e26c5e1a3e47aa5d17082cbb56
- https://git.kernel.org/stable/c/cd541f15b60e2257441398cf495d978f816d09f8
- https://git.kernel.org/linus/5cb81eeda909dbb2def209dd10636b51549a3f8a
- https://lore.kernel.org/linux-cve-announce/2026040318-CVE-2026-23458-5578@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-23458

- https://access.redhat.com/security/cve/cve-2026-23458
- https://bdu.fstec.ru/vul/2026-10895

39

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23288
BDU:2026-10896

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19.4 до 6.19.6 включительно

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23288
- https://git.kernel.org/stable/c/cca770d710d5e03bc814af585cd6975eb6d74074
- https://git.kernel.org/linus/1110a949675ebd56b3f0286e664ea543f745801c
- https://lore.kernel.org/linux-cve-announce/2026032524-CVE-2026-23288-1d11@gregkh/
- https://bdu.fstec.ru/vul/2026-10896

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23451
BDU:2026-10900

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

Уязвимый продукт: Linux: 6.19.9

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

40 **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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23451
- https://git.kernel.org/stable/c/946bb6cacf0ccada7bc80f1cfa07c1ed79511c1c
- https://git.kernel.org/stable/c/4172a7901cf43fe1cc63ef7a2ef33735ff7b7d13
- https://git.kernel.org/stable/c/9b49c854f14f5e2d493e562a1e28d2e57fe37371
- https://git.kernel.org/linus/b7405dcf7385445e10821777143f18c3ce20fa04
- https://lore.kernel.org/linux-cve-announce/2026040316-CVE-2026-23451-1298@gregkh/
- https://bdu.fstec.ru/vul/2026-10900

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31787
BDU:2026-10901

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

Уязвимый продукт: Linux: от 7.0 до 7.0.3
Red Hat Enterprise Linux: 8.4 Extended Update Support Long-Life Add-On
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

41

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

Ссылки на источник:

- https://git.kernel.org/stable/c/24daca4fc07f3ff8cd0e3f629cd982187f48436a
- https://git.kernel.org/stable/c/dbf862ce9f009128ab86b234d91413a3e450beb4
- https://git.kernel.org/stable/c/402d84ad9e89bd4cbfd07ca8598532b7021daf95
- https://git.kernel.org/stable/c/2894a351fe2ea8684919d36df3188b9a35e3926f
- https://git.kernel.org/stable/c/71bf829800758a6e3889096e4754ef47ba7fc850
- https://git.kernel.org/stable/c/2b985d3a024b9e8c24e21671b34e855569763808
- https://git.kernel.org/stable/c/446ee446d9ae66f36e95c3c90bbcc4e56b94cde0
- https://git.kernel.org/stable/c/1576ff3869cbd3620717195f971c85b7d7fd62b5
- https://lore.kernel.org/linux-cve-announce/2026043034-CVE-2026-31787-f6cc@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-31787
- https://access.redhat.com/security/cve/cve-2026-31787
- https://bdu.fstec.ru/vul/2026-10901

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31782
BDU:2026-10902

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.16 до 6.18.21 включительно
Red Hat Enterprise Linux: 10

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

42

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31782
- https://git.kernel.org/stable/c/e435a30ca6fe14c9611b1fc731c98a6d28410247
- https://git.kernel.org/stable/c/bfee04838f636d064bc92075c65c95f739003804
- https://git.kernel.org/stable/c/dbde07f06226438cd2cf1179745fa1bec5d8914a
- https://lore.kernel.org/linux-cve-announce/2026050151-CVE-2026-31782-0f2d@gregkh/
- https://access.redhat.com/security/cve/cve-2026-31782
- https://bdu.fstec.ru/vul/2026-10902

43

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8524
BDU:2026-10795

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-r4p4-x45m-mwxq
- https://issues.Google Chrome.org/issues/499565267
- https://nvd.nist.gov/vuln/detail/CVE-2026-8524
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8524
- https://security-tracker.debian.org/tracker/CVE-2026-8524
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8524

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10795

44

Краткое описание: Выполнение произвольного кода в uuid

Идентификатор уязвимости: CVE-2026-41907
BDU:2026-10885

Идентификатор программной ошибки: CWE-823 Использование для указателя смещения за пределами назначенного диапазона

Уязвимый продукт: Platform V IAM SE: до 2.3.1
uuid: до 13.0.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-23 / 2026-07-23

Ссылки на источник:

- https://github.com/uuidjs/uuid/security/advisories/GHSA-w5hq-g745-h8pq
- https://bdu.fstec.ru/vul/2026-10885

45

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-7379
BDU:2026-10848

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

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.15
Debian GNU/Linux: 13
РЕД ОС: 8.0

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

Ссылки на источник:

- https://gitlab.com/wireshark/wireshark/-/work_items/21214
- https://www.wireshark.org/security/wnpa-sec-2026-47.html
- https://security-tracker.debian.org/tracker/CVE-2026-7379
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-7379
- https://bdu.fstec.ru/vul/2026-10848

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-7376
BDU:2026-10846

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.15
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

46

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

Ссылки на источник:

- https://github.com/advisories/GHSA-qjx9-wjx4-9m8j
- https://gitlab.com/wireshark/wireshark/-/work_items/21206
- https://www.wireshark.org/security/wnpa-sec-2026-48.html
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-7376
- https://security-tracker.debian.org/tracker/CVE-2026-7376
- https://bdu.fstec.ru/vul/2026-10846

47

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8526
BDU:2026-10797

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-vrq8-3x54-8jj3
- https://issues.Google Chrome.org/issues/486536241
- https://nvd.nist.gov/vuln/detail/CVE-2026-8526
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8526
- https://security-tracker.debian.org/tracker/CVE-2026-8526
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8526

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10797

48

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8527
BDU:2026-10798

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-hj4x-332r-qxhv
- https://issues.Google Chrome.org/issues/486761172
- https://nvd.nist.gov/vuln/detail/CVE-2026-8527
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8527
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8527
- https://security-tracker.debian.org/tracker/CVE-2026-8527

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10798

Краткое описание: Получение конфиденциальной информации в Grafana

Идентификатор уязвимости: CVE-2026-42129
BDU:2026-10800

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

Уязвимый продукт: РЕД ОС: 8.0
Grafana: до 13.0.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

49

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://github.com/advisories/GHSA-f74p-cwhp-x2wx
- https://grafana.com/security/security-advisories/cve-2026-42129
- https://nvd.nist.gov/vuln/detail/CVE-2026-42129
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42129
- https://bdu.fstec.ru/vul/2026-10800

Краткое описание: Отказ в обслуживании в Grafana

Идентификатор уязвимости: CVE-2026-42127
BDU:2026-10801

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

Уязвимый продукт: РЕД ОС: 8.0
Grafana: до 13.0.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

50

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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://github.com/advisories/GHSA-3w66-95m3-8jxg
- https://grafana.com/security/security-advisories/cve-2026-42127
- https://nvd.nist.gov/vuln/detail/CVE-2026-42127
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42127
- https://bdu.fstec.ru/vul/2026-10801

51

Краткое описание: Выполнение произвольного кода в vim

Идентификатор уязвимости: CVE-2026-47162
BDU:2026-10802

Идентификатор программной ошибки: CWE-140 Некорректная нейтрализация разделителей

Уязвимый продукт: Red Hat Enterprise Linux: 10
vim: до 9.2.0495
РЕД ОС: 8.0
Red Hat OpenShift Container Platform: 4
Azure Linux: 3.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-47162
- https://bugzilla.redhat.com/show_bug.cgi?id=2487964
- https://github.com/vim/vim/commit/f08ab2f4d7d2947c8dd6c179ae08ee6146a2694b
- https://github.com/vim/vim/releases/tag/v9.2.0495
- https://github.com/vim/vim/security/advisories/GHSA-crm5-rh6j-2c7c
- https://nvd.nist.gov/vuln/detail/CVE-2026-47162
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-47162

- https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-47162.json
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47162
- https://bdu.fstec.ru/vul/2026-10802

52

Краткое описание: Отказ в обслуживании в JDBC pgjdbc

Идентификатор уязвимости: CVE-2026-42198
BDU:2026-10803

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

Уязвимый продукт: Red Hat Enterprise Linux: 10
РЕД ОС: 8.0
Red Hat AMQ Broker: 7
Red Hat build of Quarkus: 3.27.3.SP2
pgjdbc: до 42.7.11

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:19098
- https://access.redhat.com/errata/RHSA-2026:22304
- https://access.redhat.com/errata/RHSA-2026:24348
- https://access.redhat.com/errata/RHSA-2026:25030
- https://access.redhat.com/security/cve/CVE-2026-42198
- https://bugzilla.redhat.com/show_bug.cgi?id=2463857
- https://github.com/advisories/GHSA-98qh-xjc8-98pq

- https://github.com/pgjdbc/pgjdbc
- https://github.com/pgjdbc/pgjdbc/releases/tag/REL42.7.11
- https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-98qh-xjc8-98pq
- https://nvd.nist.gov/vuln/detail/CVE-2026-42198
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42198
- https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-42198.json
- https://access.redhat.com/security/cve/cve-2026-42198
- https://bdu.fstec.ru/vul/2026-10803

53

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-7378
BDU:2026-10847

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

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.15
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/advisories/GHSA-wf2x-x8pr-mjh7
- https://gitlab.com/wireshark/wireshark/-/work_items/21207
- https://www.wireshark.org/security/wnpa-sec-2026-49.html
- https://security-tracker.debian.org/tracker/CVE-2026-7378
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-7378
- https://bdu.fstec.ru/vul/2026-10847

54

Краткое описание: Получение конфиденциальной информации в mako

Идентификатор уязвимости: CVE-2026-44307
BDU:2026-10805

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

Уязвимый продукт: РЕД ОС: 8.0
mako: до 1.3.12

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-2h4p-vjrc-8xpq
- https://github.com/sqlalchemy/mako
- https://github.com/sqlalchemy/mako/commit/72e10c573ca0fbcbddd4455abca8ce92a61780d7
- https://github.com/sqlalchemy/mako/issues/435
- https://github.com/sqlalchemy/mako/releases/tag/rel_1_3_12
- https://github.com/sqlalchemy/mako/security/advisories/GHSA-2h4p-vjrc-8xpq
- https://nvd.nist.gov/vuln/detail/CVE-2026-44307
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-44307
- https://bdu.fstec.ru/vul/2026-10805

55

Краткое описание: Отказ в обслуживании в Unbound

Идентификатор уязвимости: CVE-2026-41292
BDU:2026-10807

Идентификатор программной ошибки: CWE-1010 Аутентификация

Уязвимый продукт: Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
РЕД ОС: 8.0
Unbound: до 1.25.1
Red Hat OpenStack Platform: 18.0
Red Hat Data Grid: 8
Red Hat JBoss Enterprise Application Platform Expansion Pack: -
Red Hat OpenShift Container Platform: 4
Red Hat Hardened Images: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-41292
- https://bugzilla.redhat.com/show_bug.cgi?id=2480125
- https://github.com/advisories/GHSA-2wvj-gvc7-gfhx

- https://nvd.nist.gov/vuln/detail/CVE-2026-41292
- https://redos.red-soft.ru/support/secure/
- https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-41292.json
- https://www.nlnetlabs.nl/downloads/unbound/CVE-2026-41292.txt
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-41292
- https://access.redhat.com/security/cve/cve-2026-41292
- https://security-tracker.debian.org/tracker/CVE-2026-41292
- https://bdu.fstec.ru/vul/2026-10807

56

Краткое описание: Отказ в обслуживании в Pillow

Идентификатор уязвимости: CVE-2026-42311
BDU:2026-10818

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Pillow: до 12.2.0
Debian GNU/Linux: 13
РЕД ОС: 8.0
Red Hat Quay: 3
Red Hat Ansible Automation Platform: 2
Red Hat Enterprise Linux AI: 3
Red Hat OpenShift Lightspeed: -
Red Hat AI Inference Server: 3.3
Red Hat OpenShift AI: -
Exploit Intelligence: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-pwv6-vv43-88gr
- https://github.com/python-pillow/Pillow

- https://github.com/python-pillow/Pillow/commit/58f9a1d166dcb0c274807d4423522d205b0c35ea
- https://github.com/python-pillow/Pillow/pull/9520
- https://github.com/python-pillow/Pillow/releases/tag/12.2.0
- https://github.com/python-pillow/Pillow/security/advisories/GHSA-pwv6-vv43-88gr
- https://nvd.nist.gov/vuln/detail/CVE-2026-42311
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42311
- https://security-tracker.debian.org/tracker/CVE-2026-42311
- https://access.redhat.com/security/cve/cve-2026-42311
- https://bdu.fstec.ru/vul/2026-10818

57

Краткое описание: Получение конфиденциальной информации в mako

Идентификатор уязвимости: CVE-2026-41205
BDU:2026-10804

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

Уязвимый продукт: РЕД ОС: 8.0
mako: до 1.3.11

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://github.com/advisories/GHSA-v92g-xgxw-vvmm
- https://github.com/pypa/advisory-database/tree/main/vulns/mako/PYSEC-2026-88.yaml
- https://github.com/sqlalchemy/mako
- https://github.com/sqlalchemy/mako/commit/e05ac61989a7fb9dd7dcde6cfd72dc48328719a3
- https://github.com/sqlalchemy/mako/releases/tag/rel_1_3_11
- https://github.com/sqlalchemy/mako/security/advisories/GHSA-v92g-xgxw-vvmm
- https://nvd.nist.gov/vuln/detail/CVE-2026-41205
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-41205
- https://bdu.fstec.ru/vul/2026-10804

58

Краткое описание: Получение конфиденциальной информации в python-dulwich

Идентификатор уязвимости: CVE-2026-52726
BDU:2026-10820

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

Уязвимый продукт: Red Hat Enterprise Linux: 8
OpenShift Container Platform: 4
РЕД ОС: 8.0
Red Hat Ansible Automation Platform: 2
OpenShift AI: -
python-dulwich: до 1.2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-gfhv-vqv2-4544
- https://github.com/jelmer/dulwich
- https://github.com/jelmer/dulwich/releases/tag/dulwich-1.2.5
- https://github.com/jelmer/dulwich/security/advisories/GHSA-gfhv-vqv2-4544
- https://nvd.nist.gov/vuln/detail/CVE-2026-52726
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-52726

- https://access.redhat.com/security/cve/cve-2026-52726
- https://bdu.fstec.ru/vul/2026-10820

59

Краткое описание: Обход безопасности в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-55040
BDU:2026-10845

Идентификатор программной ошибки: CWE-1038 Небезопасная автоматическая оптимизация

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040
- https://www.rapid7.com/blog/post/ra-microsoft-sharepoint-jwt-token-authentication-bypass-cve-2026-55040/
- https://bdu.fstec.ru/vul/2026-10845

60

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-7375
BDU:2026-10844

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

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.15
Debian GNU/Linux: 13
РЕД ОС: 8.0

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

Ссылки на источник:

- https://github.com/advisories/GHSA-q392-394v-mxrh
- https://gitlab.com/wireshark/wireshark/-/work_items/21225
- https://www.wireshark.org/security/wnpa-sec-2026-50.html
- https://security-tracker.debian.org/tracker/CVE-2026-7375
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-7375
- https://bdu.fstec.ru/vul/2026-10844

61

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-6868
BDU:2026-10843

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.15
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/advisories/GHSA-3cr4-47vg-rm82
- https://gitlab.com/wireshark/wireshark/-/work_items/21185
- https://www.wireshark.org/security/wnpa-sec-2026-46.html
- https://security-tracker.debian.org/tracker/CVE-2026-6868
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-6868
- https://bdu.fstec.ru/vul/2026-10843

Краткое описание: Выполнение произвольного кода в ImageMagick

Идентификатор уязвимости: CVE-2026-56370
BDU:2026-10840

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: ImageMagick: до 6.9.13-44
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

62

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

Ссылки на источник:

- https://github.com/advisories/GHSA-pmpg-6pww-fg6q
- https://github.com/ImageMagick/ImageMagick
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-pmpg-6pww-fg6q
- https://www.vulncheck.com/advisories/imagemagick-out-of-bounds-access-in-connectedcomponentsimage-via-connected-components-artifact
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-56370
- https://security-tracker.debian.org/tracker/CVE-2026-56370
- https://github.com/ImageMagick/ImageMagick/commit/2ab24d74865ab92faeeefe0fec890abf1e88e57c
- https://github.com/ImageMagick/ImageMagick6/commit/60b4e60841b429d719c59144e2505c8b0135367d

- https://bdu.fstec.ru/vul/2026-10840

63

Краткое описание: Обход безопасности в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-55034
BDU:2026-10837

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

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 8.7 AV:N/AC:L/PR:L/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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55034
- https://bdu.fstec.ru/vul/2026-10837

64

Краткое описание: Межсайтовый скриптинг в Gitea

Идентификатор уязвимости: CVE-2026-28737
BDU:2026-10838

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

Уязвимый продукт: РЕД ОС: 8.0
Gitea: от 1.25.0 до 1.26.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.7 AV:N/AC:L/PR:L/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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://github.com/go-gitea/gitea/security/advisories/GHSA-9cpj-qc93-vw8v
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-10838

65

Краткое описание: Повышение привилегий в Gitea

Идентификатор уязвимости: CVE-2026-28699
BDU:2026-10836

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.26.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://blog.gitea.com/release-of-1.26.2/
- https://github.com/go-gitea/gitea/security/advisories/GHSA-9r5x-wg6m-x2rc
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-10836

66

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-44244
BDU:2026-10828

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

Уязвимый продукт: РЕД ОС: 8.0
GitPython: до 3.1.49

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-v87r-6q3f-2j67
- https://github.com/gitpython-developers/GitPython
- https://github.com/gitpython-developers/GitPython/releases/tag/3.1.49
- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-v87r-6q3f-2j67
- https://nvd.nist.gov/vuln/detail/CVE-2026-44244
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-44244
- https://bdu.fstec.ru/vul/2026-10828

67

Краткое описание: Получение конфиденциальной информации в GitPython

Идентификатор уязвимости: CVE-2026-44243
BDU:2026-10827

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

Уязвимый продукт: РЕД ОС: 8.0
GitPython: до 3.1.48

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-7545-fcxq-7j24
- https://github.com/gitpython-developers/GitPython
- https://github.com/gitpython-developers/GitPython/releases/tag/3.1.48
- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-7545-fcxq-7j24
- https://nvd.nist.gov/vuln/detail/CVE-2026-44243
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-44243
- https://bdu.fstec.ru/vul/2026-10827

68

Краткое описание: Выполнение произвольного кода в python-dulwich

Идентификатор уязвимости: CVE-2026-42563
BDU:2026-10826

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

Уязвимый продукт: РЕД ОС: 8.0
python-dulwich: до 1.2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/advisories/GHSA-9277-mp7x-85jf
- https://github.com/jelmer/dulwich
- https://github.com/jelmer/dulwich/commit/e3331b3b3a122fc313460182f928f59723580b7b
- https://github.com/jelmer/dulwich/releases/tag/dulwich-1.2.5
- https://github.com/jelmer/dulwich/security/advisories/GHSA-9277-mp7x-85jf
- https://nvd.nist.gov/vuln/detail/CVE-2026-42563
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42563
- https://bdu.fstec.ru/vul/2026-10826

69

Краткое описание: Выполнение произвольного кода в libcaca

Идентификатор уязвимости: CVE-2026-42046
BDU:2026-10825

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

Уязвимый продукт: libcaca: до 0.99.beta20 включительно
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://github.com/cacalabs/libcaca/commit/fb77acff9ba6bb01d53940da34fb10f20b156a23
- https://github.com/cacalabs/libcaca/issues/86
- https://github.com/cacalabs/libcaca/security/advisories/GHSA-4vvg-vrqv-m56w
- https://nvd.nist.gov/vuln/detail/CVE-2026-42046
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-42046
- https://security-tracker.debian.org/tracker/CVE-2026-42046
- https://bdu.fstec.ru/vul/2026-10825

70

Краткое описание: Обход безопасности в .NET

Идентификатор уязвимости: CVE-2026-47304
BDU:2026-10971

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: .NET: от 10.0 до 10.0.10
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft Visual Studio 2017: до 15.9
Microsoft Visual Studio 2019: до 16.11
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0
Microsoft Visual Studio 2026: до 18.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47304
- https://bdu.fstec.ru/vul/2026-10971

71

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55128
BDU:2026-10968

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5561.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55128
- https://bdu.fstec.ru/vul/2026-10968

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55032
BDU:2026-10969

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5561.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

72

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55032
- https://bdu.fstec.ru/vul/2026-10969

73

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8389
BDU:2026-10970

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

Уязвимый продукт: Firefox: до 150.0.3
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://github.com/crixpwn/CVE-2026-8389
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-45/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://bdu.fstec.ru/vul/2026-10970

74

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55132
BDU:2026-10966

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20434
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5561.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5561.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20175
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55132
- https://bdu.fstec.ru/vul/2026-10966

75

Краткое описание: Отказ в обслуживании в .NET

Идентификатор уязвимости: CVE-2026-47302
BDU:2026-10972

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

Уязвимый продукт: .NET: от 10.0 до 10.0.10
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0
Microsoft Visual Studio 2026: от 18.7 до 18.7.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47302
- https://bdu.fstec.ru/vul/2026-10972

76

Краткое описание: Выполнение произвольного кода в shell-quote

Идентификатор уязвимости: CVE-2026-9277
BDU:2026-10980

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

Уязвимый продукт: Red Hat Satellite: 6.18
OpenShift Container Platform: 4.22
Red Hat Quay: 3.16
Openshift Service Mesh: 3.0
Red Hat OpenShift Virtualization: 4
Red Hat Discovery: 2
Cryostat: 4 on RHEL 9
OpenShift Dev Spaces: -
OpenShift Pipelines: -
Red Hat Developer Hub: 1.10
Red Hat OpenShift Lightspeed: -
Red Hat Build of Podman Desktop: Tech Preview
Self-service automation portal: 2
shell-quote: от 1.1.0 до 1.8.4
Cluster Observability Operator: 1.5.0
Migration Toolkit: 1.8

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://github.com/ljharb/shell-quote
- https://github.com/ljharb/shell-quote/security/advisories/GHSA-w7jw-789q-3m8p
- https://github.com/advisories/GHSA-w7jw-789q-3m8p
- https://access.redhat.com/security/cve/cve-2026-9277
- https://bdu.fstec.ru/vul/2026-10980

77

Краткое описание: Повышение привилегий в Microsoft SQL Server

Идентификатор уязвимости: CVE-2026-47295
BDU:2026-10975

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

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1125.2
Microsoft SQL Server 2022 (GDR): до 16.0.1190.2
Microsoft SQL Server 2019 (CU 32): до 15.0.4480.2
Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack: до 13.0.7095.1
Microsoft SQL Server 2017 (CU 31): до 14.0.3540.1
Microsoft SQL Server 2016 Service Pack 3 (GDR): до 13.0.6500.1
Microsoft SQL Server 2019 (GDR): до 15.0.2180.2
Microsoft SQL Server 2017 (GDR): до 14.0.2120.1
Microsoft SQL Server 2025 (CU6): до 17.0.4060.2
Microsoft SQL Server 2022 (CU 25): до 16.0.4262.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47295

- https://bdu.fstec.ru/vul/2026-10975

78

Краткое описание: Повышение привилегий в Windows GDI

Идентификатор уязвимости: CVE-2026-50387
BDU:2026-10976

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft Office: до 16.0.20228.20042
Microsoft Office LTSC 2021: до 16.111.26071215
Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Microsoft Office LTSC 2024: до 16.111.26071215
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR: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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50387
- https://bdu.fstec.ru/vul/2026-10976

79

Краткое описание: Отказ в обслуживании в Windows Active Directory Federation Services

Идентификатор уязвимости: CVE-2026-50368
BDU:2026-10977

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows Server 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-24 / 2026-07-24

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50368
- https://bdu.fstec.ru/vul/2026-10977

Краткое описание: Выполнение произвольного кода в Scramble

Идентификатор уязвимости: CVE-2026-44262
BDU:2026-10979

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

Уязвимый продукт: Scramble: от 0.13.2 до 0.13.22

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

80

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://github.com/dedoc/scramble/security/advisories/GHSA-4rm2-28vj-fj39
- https://github.com/dedoc/scramble/releases/tag/v0.13.22
- https://www.sentinelone.com/vulnerability-database/CVE-2026-44262/
- https://mallory.ai/vulnerabilities/CVE-2026-44262
- https://github.com/akash-osmsec/CVE-2026-44262-
- https://github.com/joshuavanderpoll/CVE-2026-44262
- https://bdu.fstec.ru/vul/2026-10979

81

Краткое описание: Выполнение произвольного кода в DbGate

Идентификатор уязвимости: CVE-2026-47668
BDU:2026-10981

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

Уязвимый продукт: DbGate: до 7.1.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://github.com/dbgate/dbgate/security/advisories/GHSA-8v3q-9vmx-36vc
- https://github.com/runZeroInc/nuclei-templates/blob/main/http/vulnerabilities/dbgate-unauth-rce.yaml
- https://github.com/dbgate/dbgate/releases/tag/v7.1.9
- https://www.dbgate.ru/
- https://github.com/Nxploited/CVE-2026-47668
- https://docs.devguard.org/vulnerability-database/CVE-2026-47668/
- https://github.com/projectdiscovery/nuclei-templates/pull/16221
- https://mallory.ai/vulnerabilities/CVE-2026-47668
- https://bdu.fstec.ru/vul/2026-10981

82

Краткое описание: Отказ в обслуживании в Azure Active Directory

Идентификатор уязвимости: CVE-2026-50653
BDU:2026-10965

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

Уязвимый продукт: Azure Active Directory: до 8.19.2
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50653
- https://bdu.fstec.ru/vul/2026-10965

83

Краткое описание: Повышение привилегий в Windows Runtime

Идентификатор уязвимости: CVE-2026-58527
BDU:2026-10973

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

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8875
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58527
- https://bdu.fstec.ru/vul/2026-10973

84

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8390
BDU:2026-10954

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Firefox: до 150.0.3
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.5 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-45/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://bdu.fstec.ru/vul/2026-10954

85

Краткое описание: Повышение привилегий в .NET

Идентификатор уязвимости: CVE-2026-50650
BDU:2026-10962

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

Уязвимый продукт: .NET: от 9.0 до 9.0.18
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0
Microsoft Visual Studio 2026: от 18.7 до 18.7.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50650
- https://bdu.fstec.ru/vul/2026-10962

86

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8529
BDU:2026-10920

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-9g6r-32x9-xm98
- https://issues.Google Chrome.org/issues/490222151
- https://nvd.nist.gov/vuln/detail/CVE-2026-8529
- https://redos.red-soft.ru/support/secure/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8529
- https://security-tracker.debian.org/tracker/CVE-2026-8529

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10920

87

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8532
BDU:2026-10921

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-phr6-cg52-w545
- https://issues.Google Chrome.org/issues/492812194
- https://nvd.nist.gov/vuln/detail/CVE-2026-8532
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8532
- https://security-tracker.debian.org/tracker/CVE-2026-8532
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8532

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10921

88

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8533
BDU:2026-10922

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-6gfv-c8p2-h6xg
- https://issues.Google Chrome.org/issues/495247950
- https://nvd.nist.gov/vuln/detail/CVE-2026-8533
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8533
- https://security-tracker.debian.org/tracker/CVE-2026-8533
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8533

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10922

89

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8534
BDU:2026-10923

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-rq48-56f4-2ww7
- https://issues.Google Chrome.org/issues/495314407
- https://nvd.nist.gov/vuln/detail/CVE-2026-8534
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8534
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8534
- https://security-tracker.debian.org/tracker/CVE-2026-8534

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10923

90

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8544
BDU:2026-10929

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-hh3h-hx57-wxhf
- https://issues.Google Chrome.org/issues/497151750
- https://nvd.nist.gov/vuln/detail/CVE-2026-8544
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8544
- https://security-tracker.debian.org/tracker/CVE-2026-8544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8544

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10929

91

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8548
BDU:2026-10931

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-39w8-2393-mh75
- https://issues.Google Chrome.org/issues/497821764
- https://nvd.nist.gov/vuln/detail/CVE-2026-8548
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8548
- https://security-tracker.debian.org/tracker/CVE-2026-8548
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8548

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10931

92

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8540
BDU:2026-10927

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-7w4v-j6pr-v8hv
- https://issues.Google Chrome.org/issues/496627235
- https://nvd.nist.gov/vuln/detail/CVE-2026-8540
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8540
- https://security-tracker.debian.org/tracker/CVE-2026-8540

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10927

93

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8551
BDU:2026-10934

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-v77q-jqj8-8vvq
- https://issues.Google Chrome.org/issues/498376171
- https://nvd.nist.gov/vuln/detail/CVE-2026-8551
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8551
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8551
- https://security-tracker.debian.org/tracker/CVE-2026-8551

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10934

94

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8557
BDU:2026-10936

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.5 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: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-wh82-47gg-p482
- https://issues.Google Chrome.org/issues/502978647
- https://nvd.nist.gov/vuln/detail/CVE-2026-8557
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8557
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8557
- https://security-tracker.debian.org/tracker/CVE-2026-8557

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10936

95

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8558
BDU:2026-10937

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-7m72-mq6q-p26x
- https://issues.Google Chrome.org/issues/503425922
- https://nvd.nist.gov/vuln/detail/CVE-2026-8558
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8558
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8558
- https://security-tracker.debian.org/tracker/CVE-2026-8558

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10937

96

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8575
BDU:2026-10941

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-pwc7-pghh-4vww
- https://issues.Google Chrome.org/issues/496217775
- https://nvd.nist.gov/vuln/detail/CVE-2026-8575
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8575
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8575
- https://security-tracker.debian.org/tracker/CVE-2026-8575

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10941

97

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-68580
BDU:2026-10946

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

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-69xf-pqrw-596x
- https://www.vulncheck.com/advisories/freerdp-before-integer-overflow-via-audio-input-channel
- https://bdu.fstec.ru/vul/2026-10946

98

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8569
BDU:2026-10960

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-m34r-5p3p-q822
- https://issues.Google Chrome.org/issues/490229299
- https://nvd.nist.gov/vuln/detail/CVE-2026-8569
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8569
- https://security-tracker.debian.org/tracker/CVE-2026-8569
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8569
- https://bdu.fstec.ru/vul/2026-10960

99

Краткое описание: Отказ в обслуживании в .NET

Идентификатор уязвимости: CVE-2026-50525
BDU:2026-10961

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

Уязвимый продукт: .NET: от 10.0 до 10.0.10
Microsoft Visual Studio 2022: от 17.12 до 17.12.22
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0
Microsoft Visual Studio 2026: от 18.7 до 18.7.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50525
- https://bdu.fstec.ru/vul/2026-10961

100

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8549
BDU:2026-10932

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70 (Chromium-based)
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-6fqp-88f8-7477
- https://issues.Google Chrome.org/issues/497985088
- https://nvd.nist.gov/vuln/detail/CVE-2026-8549
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8549
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8549
- https://security-tracker.debian.org/tracker/CVE-2026-8549

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-10932

101

Краткое описание: Обход безопасности в Langflow

Идентификатор уязвимости: CVE-2026-55255
BDU:2026-10993

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

Уязвимый продукт: Langflow: до 1.9.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/langflow-ai/langflow/security/advisories/GHSA-qrpv-q767-xqq2
- https://github.com/langflow-ai/langflow/pull/12832
- https://github.com/langflow-ai/langflow/commit/2c9f498d664a3c32698b57d7c5e752625291060e
- https://bdu.fstec.ru/vul/2026-10993

102

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67304
BDU:2026-10990

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-78jj-45vh-jpm5
- https://bdu.fstec.ru/vul/2026-10990

103

Краткое описание: Выполнение произвольного кода в Zoom Meeting SDK for Windows

Идентификатор уязвимости: CVE-2026-53412
BDU:2026-10991

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Zoom Meeting SDK for Windows: до 7.0.0
Zoom Workplace VDI Client for Windows: до 7.0.10
Zoom Workplace for Windows: до 7.0.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://www.zoom.com/en/trust/security-bulletin/zsb-26014/
- https://www.bleepingcomputer.com/news/security/zoom-warns-of-critical-account-takeover-vulnerability/
- https://bdu.fstec.ru/vul/2026-10991

104

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67298
BDU:2026-10988

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/commit/46848765f2a1134f8652f8760eefb5e85d64a9b8
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qmvw-52ph-q5pv
- https://bdu.fstec.ru/vul/2026-10988

105

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67297
BDU:2026-10987

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

Уязвимый продукт: FreeRDP: до 3.29.0

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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2c6r-4pr4-9x8m
- https://bdu.fstec.ru/vul/2026-10987

106

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67296
BDU:2026-10986

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-jm8r-22j6-4m4v
- https://bdu.fstec.ru/vul/2026-10986

107

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67291
BDU:2026-10985

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-hgj8-g595-wfc6
- https://github.com/FreeRDP/FreeRDP/commit/f3b4347105114fe7453828736bea069999af319f
- https://bdu.fstec.ru/vul/2026-10985

108

Краткое описание: Отказ в обслуживании в FreeRDP

Идентификатор уязвимости: CVE-2026-67290
BDU:2026-10984

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/commit/8d3b86022f0d71aefa7bd2e466d2d391693a41b3
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-whq8-c3v3-p8v8
- https://bdu.fstec.ru/vul/2026-10984

109

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-67289
BDU:2026-10983

Идентификатор программной ошибки: CWE-113 Некорректная нейтрализация последовательностей символов CRLF в HTTP-заголовках (расщепление HTTP-ответов)

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mwwh-mhp9-q7vm
- https://github.com/FreeRDP/FreeRDP/commit/f3b4347105114fe7453828736bea069999af319f
- https://bdu.fstec.ru/vul/2026-10983

110

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-67299
BDU:2026-10989

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: FreeRDP: до 3.29.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-34hq-hwjw-q8v3
- https://bdu.fstec.ru/vul/2026-10989

111

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9998
BDU:2026-11032

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9998
- https://security-tracker.debian.org/tracker/CVE-2026-9998
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513337118
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://github.com/George0Papasotiriou/CVE-2026-9998-Insecure-Deserialization-in-Blockchain-Oracle
- https://security-tracker.debian.org/tracker/CVE-2026-9998
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9998

- https://bdu.fstec.ru/vul/2026-11032

112

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10001
BDU:2026-11033

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10001
- https://security-tracker.debian.org/tracker/CVE-2026-10001
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513505927
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10001
- https://security-tracker.debian.org/tracker/CVE-2026-10001
- https://bdu.fstec.ru/vul/2026-11033

113

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10002
BDU:2026-11034

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10002
- https://security-tracker.debian.org/tracker/CVE-2026-10002
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513536416
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10002
- https://security-tracker.debian.org/tracker/CVE-2026-10002
- https://bdu.fstec.ru/vul/2026-11034

114

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10003
BDU:2026-11035

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-02 / 2026-08-02

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10003
- https://security-tracker.debian.org/tracker/CVE-2026-10003
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513609324
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10003
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10003
- https://bdu.fstec.ru/vul/2026-11035

115

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10006
BDU:2026-11037

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-02 / 2026-08-02

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10006
- https://security-tracker.debian.org/tracker/CVE-2026-10006
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513750691
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10006
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10006

- https://bdu.fstec.ru/vul/2026-11037

116

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10007
BDU:2026-11038

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10007
- https://security-tracker.debian.org/tracker/CVE-2026-10007
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513754619
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10007
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10007
- https://bdu.fstec.ru/vul/2026-11038

117

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10009
BDU:2026-11039

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-02 / 2026-08-02

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10009
- https://security-tracker.debian.org/tracker/CVE-2026-10009
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513973560
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10009
- https://security-tracker.debian.org/tracker/CVE-2026-10009
- https://bdu.fstec.ru/vul/2026-11039

118

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10013
BDU:2026-11044

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10013
- https://security-tracker.debian.org/tracker/CVE-2026-10013
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/514715455
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10013
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10013
- https://bdu.fstec.ru/vul/2026-11044

119

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10012
BDU:2026-11043

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10012
- https://security-tracker.debian.org/tracker/CVE-2026-10012
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/514063977
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10012
- https://security-tracker.debian.org/tracker/CVE-2026-10012
- https://bdu.fstec.ru/vul/2026-11043

120

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10015
BDU:2026-11045

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10015
- https://security-tracker.debian.org/tracker/CVE-2026-10015
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/514746176
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10015
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10015
- https://bdu.fstec.ru/vul/2026-11045

121

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10016
BDU:2026-11046

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10016
- https://security-tracker.debian.org/tracker/CVE-2026-10016
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/515155946
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10016
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10016
- https://bdu.fstec.ru/vul/2026-11046

122

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10017
BDU:2026-11047

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10017
- https://security-tracker.debian.org/tracker/CVE-2026-10017
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504156069
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10017
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10017
- https://bdu.fstec.ru/vul/2026-11047

123

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10019
BDU:2026-11049

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10019
- https://security-tracker.debian.org/tracker/CVE-2026-10019
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/505056913
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10019
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10019
- https://bdu.fstec.ru/vul/2026-11049

124

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10021
BDU:2026-11050

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10021
- https://security-tracker.debian.org/tracker/CVE-2026-10021
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/497327715
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-10021
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10021
- https://bdu.fstec.ru/vul/2026-11050

125

Краткое описание: Получение конфиденциальной информации в MediaWiki

Идентификатор уязвимости: CVE-2026-34092
BDU:2026-11025

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

Уязвимый продукт: MediaWiki: от 1.45.0 до 1.45.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://phabricator.wikimedia.org/T384147
- https://security-tracker.debian.org/tracker/CVE-2026-34092
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11025

126

Краткое описание: Получение конфиденциальной информации в MediaWiki

Идентификатор уязвимости: CVE-2026-34091
BDU:2026-11024

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

Уязвимый продукт: Ubuntu: 26.04 LTS
с: от 1.45.0 до 1.45.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://phabricator.wikimedia.org/T411305
- https://security-tracker.debian.org/tracker/CVE-2026-34091
- https://ubuntu.com/security/CVE-2026-34091
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11024

127

Краткое описание: Получение конфиденциальной информации в MediaWiki

Идентификатор уязвимости: CVE-2026-34088
BDU:2026-11022

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

Уязвимый продукт: Ubuntu: 24.04 LTS
MediaWiki: от 1.45.0 до 1.45.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://phabricator.wikimedia.org/T410429
- https://security-tracker.debian.org/tracker/CVE-2026-34088
- https://ubuntu.com/security/CVE-2026-34088
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11022

128

Краткое описание: Получение конфиденциальной информации в GitPython

Идентификатор уязвимости: CVE-2026-67322
BDU:2026-10998

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

Уязвимый продукт: GitPython: до 3.1.52

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-rwj8-pgh3-r573
- https://bdu.fstec.ru/vul/2026-10998

129

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-67323
BDU:2026-10999

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: GitPython: до 3.1.51

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-956x-8gvw-wg5v
- https://bdu.fstec.ru/vul/2026-10999

130

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-67324
BDU:2026-11000

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

Уязвимый продукт: GitPython: до 3.1.51

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-v396-v7q4-x2qj
- https://bdu.fstec.ru/vul/2026-11000

131

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-67325
BDU:2026-11001

Идентификатор программной ошибки: CWE-184 Неполный черный список

Уязвимый продукт: GitPython: до 3.1.51

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-2f96-g7mh-g2hx
- https://bdu.fstec.ru/vul/2026-11001

132

Краткое описание: Выполнение произвольного кода в Sequelize

Идентификатор уязвимости: CVE-2026-69240
BDU:2026-11009

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

Уязвимый продукт: Sequelize: до 6.37.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/sequelize/sequelize/security/advisories/GHSA-v8fg-2rw7-q452
- https://github.com/sequelize/sequelize/commit/5deadd2410ae9136a21fb652db206d27bb715f26
- https://github.com/sequelize/sequelize/releases/tag/v6.37.4
- https://bdu.fstec.ru/vul/2026-11009

133

Краткое описание: Отказ в обслуживании в cryptography

Идентификатор уязвимости: CVE-2026-69249
BDU:2026-11011

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

Уязвимый продукт: cryptography: от 48.0.0 до 49.0.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/pyca/cryptography/security/advisories/GHSA-jwv3-5hgf-82ww
- https://github.com/pyca/cryptography/pull/14960
- https://github.com/pyca/cryptography/commit/4a12cf49675a184e47f912b00b04f3a629283582
- https://github.com/pyca/cryptography/tags
- https://bdu.fstec.ru/vul/2026-11011

134

Краткое описание: Отказ в обслуживании в Libexif

Идентификатор уязвимости: CVE-2026-32775
BDU:2026-11014

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

Уязвимый продукт: Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
РЕД ОС: 8.0
Libexif: до 0.6.25 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.8 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: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/libexif/libexif/issues/247
- https://github.com/libexif/libexif/commit/7df372e9d31d7c993a22b913c813a5f7ec4f3692
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://access.redhat.com/security/cve/cve-2026-32775
- https://security-tracker.debian.org/tracker/CVE-2026-32775
- https://bdu.fstec.ru/vul/2026-11014

Краткое описание: Отказ в обслуживании в Unbound

Идентификатор уязвимости: CVE-2026-33278
BDU:2026-11016

Идентификатор программной ошибки: CWE-672 Использование ресурса после окончания срока его действия или освобождения

Уязвимый продукт: Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
OpenShift Container Platform: 4
РЕД ОС: 8.0
Unbound: от 1.19.1 до 1.25.1
Red Hat Hardened Images: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://www.nlnetlabs.nl/downloads/unbound/CVE-2026-33278.txt
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://access.redhat.com/security/cve/cve-2026-33278
- https://security-tracker.debian.org/tracker/CVE-2026-33278
- https://bdu.fstec.ru/vul/2026-11016

136

Краткое описание: Повышение привилегий в MinIO

Идентификатор уязвимости: CVE-2026-33322
BDU:2026-11017

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: РЕД ОС: 8.0
MinIO: от RELEASE.2022-11-08T05-27-07Z до RELEASE.2026-03-17T21-25-16Z

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/minio/minio/security/advisories/GHSA-5cx5-wh4m-82fh
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11017

137

Краткое описание: Получение конфиденциальной информации в MinIO

Идентификатор уязвимости: CVE-2026-33419
BDU:2026-11018

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: РЕД ОС: 8.0
MinIO: от RELEASE.2026-03-17T21-25-16Z до RELEASE.2026-03-17T21-25-16Z

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/minio/minio/security/advisories/GHSA-jv87-32hw-hh99
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11018

138

Краткое описание: Повышение привилегий в Glances

Идентификатор уязвимости: CVE-2026-33641
BDU:2026-11020

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

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-07-31 / 2026-07-31

Ссылки на источник:

- https://github.com/nicolargo/glances/security/advisories/GHSA-qhj7-v7h7-q4c7
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11020

139

Краткое описание: Получение конфиденциальной информации в MediaWiki

Идентификатор уязвимости: CVE-2026-34087
BDU:2026-11023

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

Уязвимый продукт: Ubuntu: 26.04 LTS
MediaWiki: от 1.45.0 до 1.45.2
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://phabricator.wikimedia.org/T412061
- https://security-tracker.debian.org/tracker/CVE-2026-34087
- https://ubuntu.com/security/CVE-2026-34087
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-11023

140

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-10022
BDU:2026-11051

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-02 / 2026-08-02

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-10022
- https://security-tracker.debian.org/tracker/CVE-2026-10022
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513289241
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10022
- https://security-tracker.debian.org/tracker/CVE-2026-10022
- https://bdu.fstec.ru/vul/2026-11051