НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-09-04.1 | 4 сентября 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-62887	Windows NTFS	Локальный	OSI	2026-08-13	✓
2	Высокая	CVE-2026-23136	Linux	Сетевой	DoS	2026-08-05	✓
3	Высокая	CVE-2026-43307	Linux	Локальный	ACE	2026-07-28	✓
4	Высокая	CVE-2026-43222	Linux	Локальный	ACE	2026-07-28	✓
5	Высокая	CVE-2026-43297	Linux	Смежная сеть	ACE	2026-07-28	✓
6	Высокая	CVE-2026-46259	Linux	Локальный	DoS	2026-08-05	✓
7	Высокая	CVE-2026-46270	Linux	Локальный	DoS	2026-08-05	✓
8	Высокая	CVE-2026-46267	Linux	Локальный	DoS	2026-08-05	✓
9	Высокая	CVE-2026-46265	Linux	Сетевой	DoS	2026-08-05	✓
10	Высокая	CVE-2026-46253	Linux	Локальный	DoS	2026-08-05	✓
11	Высокая	CVE-2026-23148	Linux	Сетевой	DoS	2026-08-05	✓
12	Высокая	CVE-2026-46323	Linux	Смежная сеть	DoS	2026-08-05	✓
13	Высокая	CVE-2026-23158	Linux	Локальный	ACE	2026-08-05	✓

14	Высокая	CVE-2026-39304	Apache ActiveMQ	Сетевой	DoS	2026-08-17	✓
15	Высокая	CVE-2026-23223	Linux	Локальный	ACE	2026-08-05	✓
16	Высокая	CVE-2026-23233	Linux	Локальный	ACE	2026-08-04	✓
17	Высокая	CVE-2026-23344	Linux	Смежная сеть	ACE	2026-08-11	✓
18	Высокая	CVE-2026-23387	Linux	Локальный	ACE	2026-08-12	✓
19	Высокая	CVE-2026-23390	Linux	Смежная сеть	ACE	2026-08-11	✓
20	Высокая	CVE-2026-64907	Microsoft Office Word	Локальный	ACE	2026-08-14	✓
21	Критическая	CVE-2026-53434	Apache Tomcat	Сетевой	DoS	2026-08-14	✓
22	Критическая	CVE-2026-55276	Apache Tomcat	Сетевой	OSI	2026-08-14	✓
23	Высокая	CVE-2026-29129	Apache Tomcat	Сетевой	SB	2026-08-14	✓
24	Высокая	CVE-2026-40466	Apache ActiveMQ	Сетевой	ACE	2026-08-17	✓
25	Высокая	CVE-2026-46251	Linux	Локальный	DoS	2026-08-05	✓
26	Высокая	CVE-2026-42403	Apache Neethi	Сетевой	DoS	2026-08-14	✓
27	Высокая	CVE-2026-42402	Apache Neethi	Сетевой	DoS	2026-08-14	✓
28	Высокая	CVE-2026-23200	Linux	Локальный	ACE	2026-08-07	✓

29	Высокая	CVE-2026-45984	Linux	Локальный	DoS	2026-08-05	✓
30	Высокая	CVE-2026-43278	Linux	Локальный	DoS	2026-08-05	✓
31	Высокая	CVE-2026-45970	Linux	Локальный	DoS	2026-08-05	✓
32	Высокая	CVE-2026-23230	Linux	Сетевой	DoS	2026-08-05	✓
33	Высокая	CVE-2026-23242	Linux	Сетевой	DoS	2026-08-05	✓
34	Высокая	CVE-2026-23243	Linux	Локальный	DoS	2026-08-05	✓
35	Высокая	CVE-2026-23268	Linux	Локальный	DoS	2026-08-05	✓
36	Высокая	CVE-2026-23272	Linux	Локальный	DoS	2026-08-05	✓
37	Высокая	CVE-2026-23273	Linux	Локальный	DoS	2026-08-05	✓
38	Высокая	CVE-2026-43128	Linux	Локальный	DoS	2026-08-05	✓
39	Высокая	CVE-2026-43134	Linux	Смежная сеть	CI	2026-08-05	✓
40	Высокая	CVE-2026-43158	Linux	Сетевой	DoS	2026-08-05	✓
41	Высокая	CVE-2026-43180	Linux	Локальный	DoS	2026-08-05	✓
42	Высокая	CVE-2026-43184	Linux	Сетевой	OSI	2026-08-05	✓
43	Высокая	CVE-2026-43187	Linux	Сетевой	DoS	2026-08-05	✓

44	Высокая	CVE-2026-43205	Linux	Локальный	DoS	2026-08-05	✓
45	Высокая	CVE-2026-43212	Linux	Локальный	DoS	2026-08-05	✓
46	Высокая	CVE-2026-43226	Linux	Сетевой	DoS	2026-08-05	✓
47	Высокая	CVE-2026-68138	Linux	Локальный	DoS	2026-08-17	✓
48	Высокая	CVE-2026-73620	GitPython	Сетевой	OSI	2026-08-17	✓
49	Высокая	CVE-2026-73623	GitPython	Сетевой	ACE	2026-08-17	✓
50	Высокая	CVE-2026-43279	Linux	Локальный	DoS	2026-08-05	✓
51	Высокая	CVE-2026-43283	Linux	Локальный	DoS	2026-08-05	✓
52	Высокая	CVE-2026-43291	Linux	Смежная сеть	DoS	2026-08-05	✓
53	Высокая	CVE-2026-43296	Linux	Сетевой	DoS	2026-08-05	✓
54	Высокая	CVE-2026-45852	Linux	Локальный	DoS	2026-08-05	✓
55	Высокая	CVE-2026-45860	Linux	Сетевой	DoS	2026-08-05	✓
56	Высокая	CVE-2026-45862	Linux	Локальный	DoS	2026-08-05	✓
57	Высокая	CVE-2026-45935	Linux	Локальный	DoS	2026-08-05	✓
58	Высокая	CVE-2026-45946	Linux	Локальный	DoS	2026-08-05	✓

59	Критическая	CVE-2026-45972	Linux	Сетевой	DoS	2026-08-05	✓
60	Высокая	CVE-2026-15226	Ubuntu	Локальный	PE	2026-08-04	✓
61	Высокая	CVE-2026-56368	ImageMagick	Сетевой	DoS	2026-07-21	✓
62	Высокая	CVE-2026-53461	ImageMagick	Сетевой	DoS	2026-07-21	✓
63	Высокая	CVE-2026-55994	Apache Camel	Сетевой	OSI	2026-07-16	✓
64	Высокая	CVE-2026-55993	Apache Camel	Сетевой	OSI	2026-07-16	✓
65	Высокая	CVE-2026-64600	Linux	Локальный	ACE	2026-07-23	✓
66	Высокая	CVE-2026-55044	Office Online Server	Локальный	ACE	2026-07-16	✓
67	Высокая	CVE-2026-50411	Windows Active Directory Federation Services	Сетевой	DoS	2026-07-16	✓
68	Высокая	CVE-2026-50685	Windows DHCP Server	Сетевой	ACE	2026-07-16	✓
69	Высокая	CVE-2026-50686	Windows OLE	Сетевой	ACE	2026-07-16	✓
70	Высокая	CVE-2026-50688	Windows Win32k	Локальный	PE	2026-07-16	✓
71	Высокая	CVE-2026-50689	Windows Clipboard Server	Локальный	PE	2026-07-16	✓
72	Критическая	CVE-2026-56190	Remote Desktop Protocol	Сетевой	ACE	2026-07-16	✓
73	Высокая	CVE-2026-24308	ZooKeeper	Сетевой	OSI	2026-07-23	✓

74	Критическая	CVE-2026-20706	Gitea	Сетевой	PE	2026-07-27	✓
75	Высокая	CVE-2026-55055	Windows Active Directory Federation Services	Локальный	ACE	2026-07-16	✓
76	Высокая	CVE-2026-56819	Netty	Сетевой	DoS	2026-07-27	✓
77	Высокая	CVE-2026-66373	Redis	Сетевой	ACE	2026-07-27	✓
78	Критическая	CVE-2026-16723	FastJson	Сетевой	ACE	2026-07-27	✓
79	Критическая	CVE-2026-16232	Check Point SmartConsole	Сетевой	ACE	2026-07-27	✓
80	Высокая	CVE-2023-53751	Linux	Сетевой	ACE	2026-07-21	✓
81	Высокая	CVE-2026-23234	Linux	Смежная сеть	ACE	2026-07-21	✓
82	Высокая	CVE-2026-29079	Lexbor	Сетевой	DoS	2026-03-10	✓
83	Критическая	CVE-2026-48204	Apache Camel	Сетевой	RLF	2026-07-16	✓
84	Высокая	CVE-2026-58635	Windows Narrator Braille	Локальный	PE	2026-07-28	✓
85	Высокая	CVE-2026-50454	Windows User Interface Core	Локальный	PE	2026-07-28	✓
86	Высокая	CVE-2026-54992	Microsoft Message Queuing Queue Manager	Локальный	ACE	2026-07-28	✓
87	Высокая	CVE-2023-54207	Linux	Локальный	ACE	2026-07-21	✓

88	Критическая	CVE-2026-41179	Rclone	Сетевой	ACE	2026-07-29	✓
89	Критическая	CVE-2026-59827	Metabase	Сетевой	ACE	2026-07-29	✓
90	Критическая	CVE-2026-51302	SQLite	Сетевой	ACE	2026-07-29	✓
91	Критическая	CVE-2026-51303	SQLite	Сетевой	ACE	2026-07-29	✓
92	Критическая	CVE-2026-27641	Flask-Reuploaded	Сетевой	ACE	2026-07-29	✓
93	Критическая	CVE-2026-53921	OpenWrt	Сетевой	ACE	2026-07-29	✓
94	Высокая	CVE-2026-51297	SQLite	Сетевой	ACE	2026-07-29	✓
95	Высокая	CVE-2026-51296	SQLite	Сетевой	ACE	2026-07-29	✓
96	Высокая	CVE-2026-53366	Linux	Локальный	DoS	2026-07-29	✓
97	Критическая	CVE-2026-16812	VMware SD-WAN Orchestrator	Сетевой	ACE	2026-07-29	✓
98	Критическая	CVE-2026-51300	SQLite	Сетевой	DoS	2026-07-29	✓
99	Высокая	CVE-2026-51304	SQLite	Сетевой	ACE	2026-07-29	✓
100	Критическая	CVE-2026-31669	Linux	Сетевой	ACE	2026-07-22	✓
101	Критическая	CVE-2026-31668	Linux	Сетевой	DoS	2026-07-22	✓
102	Критическая	CVE-2026-31657	Linux	Сетевой	DoS	2026-07-22	✓

103	Высокая	CVE-2026-23191	Linux	Локальный	DoS	2026-07-23	✓
104	Высокая	CVE-2026-31785	Linux	Смежная сеть	ACE	2026-07-23	✓
105	Высокая	CVE-2026-31748	Linux	Смежная сеть	ACE	2026-07-23	✓
106	Высокая	CVE-2026-31735	Linux	Локальный	ACE	2026-07-23	✓
107	Высокая	CVE-2026-55141	Office Online Server	Локальный	ACE	2026-07-30	✓
108	Критическая	CVE-2026-56159	DHCP Server Service	Сетевой	ACE	2026-07-30	✓
109	Высокая	CVE-2026-58530	Windows Resilient File System	Локальный	ACE	2026-07-30	✓
110	Критическая	CVE-2026-31705	Linux	Сетевой	ACE	2026-07-22	✓
111	Высокая	CVE-2026-50367	Windows Sensor Data Service	Локальный	PE	2026-07-30	✓
112	Высокая	CVE-2026-49783	Windows Secure Boot	Локальный	SB	2026-07-30	✓
113	Высокая	CVE-2026-50655	Microsoft Windows Media Foundation	Локальный	ACE	2026-07-30	✓
114	Высокая	CVE-2026-50476	Windows Network Connections Service	Локальный	PE	2026-07-30	✓
115	Высокая	CVE-2026-50435	Windows Overlay Filter	Локальный	PE	2026-07-30	✓
116	Высокая	CVE-2026-58632	Windows Win32 Kernel Subsystem	Локальный	PE	2026-07-30	✓
117	Высокая	CVE-2026-56176	Windows Win32k	Локальный	PE	2026-07-30	✓

118	Высокая	CVE-2026-49181	Windows DHCP Client	Сетевой	PE	2026-07-30	✓
119	Высокая	CVE-2026-31747	Linux	Смежная сеть	ACE	2026-07-23	✓
120	Высокая	CVE-2026-43379	Linux	Сетевой	ACE	2026-07-22	✓
121	Критическая	CVE-2026-43011	Linux	Сетевой	ACE	2026-07-22	✓
122	Высокая	BDU:2026-10684	PT Application Inspector (PT AI)	Сетевой	ACE	2026-07-30	✓
123	Критическая	CVE-2026-31718	Linux	Сетевой	ACE	2026-07-22	✓
124	Критическая	CVE-2026-23450	Linux	Сетевой	ACE	2026-07-22	✓
125	Высокая	CVE-2026-54107	Windows Win32k	Локальный	PE	2026-07-30	✓
126	Критическая	CVE-2026-59243	Airflow Fab Provider	Сетевой	PE	2026-07-30	✓
127	Высокая	CVE-2026-67215	cJSON	Сетевой	DoS	2026-07-30	✓
128	Критическая	CVE-2026-60004	Gitea	Сетевой	ACE	2026-07-30	✓
129	Критическая	CVE-2026-58025	MediaWiki	Сетевой	ACE	2026-07-30	✓
130	Критическая	CVE-2026-66066	Ruby on Rails	Сетевой	ACE	2026-07-30	✓

1

Краткое описание: Получение конфиденциальной информации в Windows NTFS

Идентификатор уязвимости: CVE-2026-62887
BDU:2026-11619

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26200.9106
Windows Server 2012: до 6.2.9200.26280
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 (Server Core installation): до 6.2.9200.26280
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9115
Windows Server 2019 (Server Core installation): до 10.0.17763.9115
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/advisory/CVE-2026-62887
- https://bdu.fstec.ru/vul/2026-11619

2

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23136
BDU:2026-11828

Идентификатор программной ошибки: CWE-371 Уязвимости, связанные с состоянием

Уязвимый продукт: Linux: от 6.6 до 6.6.120 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://git.kernel.org/stable/c/10b7c72810364226f7b27916ea3e2a4f870bc04b
- https://git.kernel.org/stable/c/90a60fe61908afa0eaf7f8fcf1421b9b50e5f7ff
- https://git.kernel.org/stable/c/e94075e950a6598e710b9f7dffea5aa388f40313
- https://www.cve.org/CVERecord?id=CVE-2026-23136
- https://git.kernel.org/linus/11194b416ef95012c2cfe5f546d71af07b639e93
- https://security-tracker.debian.org/tracker/CVE-2026-23136
- https://access.redhat.com/security/cve/CVE-2026-23136

- https://ubuntu.com/security/CVE-2026-23136
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11828

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43307
BDU:2026-11814

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

Уязвимый продукт: Linux: от 6.12 до 6.12.74 включительно
Astra Linux Special Edition: 4.8

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.

3

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

Ссылки на источник:

- https://git.kernel.org/stable/c/f42ddb2945ae4ce2b6f1c2e7aae9f14455a734d3
- https://www.cve.org/CVERecord?id=CVE-2026-43307
- https://git.kernel.org/stable/c/a40f316085985f916ba1599fc303fdbc6a078e86
- https://git.kernel.org/stable/c/a8e88edfd69df7b63c882aa53e61e7c078806ad7
- https://git.kernel.org/linus/c1b14015224cfcccd5356333763f2f4f401bd810
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11814

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43222
BDU:2026-11815

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 6.5 до 6.6.127 включительно
Astra Linux Special Edition: 4.8

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.

4 **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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43222
- https://git.kernel.org/stable/c/a5b1ddbe31f49b4da78642157589970e9b60a231
- https://git.kernel.org/stable/c/34f36f9c6114af781a5a4f7a7c99334c85b73fc7
- https://git.kernel.org/stable/c/f122f2b3ce9dbde60bf7ab0b180fe4a01f9d9bc4
- https://git.kernel.org/stable/c/74abfadd7ef5ac9f3a6111d550cc651d1457c641
- https://git.kernel.org/linus/a505ca2db89ad92a8d8d27fa68ebafb12e04a679
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11815

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43297
BDU:2026-11813

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.8 до 6.12.74 включительно
Astra Linux Special Edition: 4.8

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.

5

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43297
- https://git.kernel.org/stable/c/5da29ade540b51763b950987bd410add7edaf3d1
- https://git.kernel.org/stable/c/1af2853b4e97fd95262fdef311b2334337069bc9
- https://git.kernel.org/stable/c/aa22221c5dc695a3d479e1e1b63f0c0e9eb29dbf
- https://git.kernel.org/linus/81f8e0e6a2e115df9274d0289779f8fca694479c
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11813

6

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46259
BDU:2026-11805

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 2.6.26 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46259
- https://security-tracker.debian.org/tracker/CVE-2026-46259
- https://git.kernel.org/linus/76149d53502cf17ef3ae454ff384551236fba867
- https://git.kernel.org/stable/c/0e64bd46a04a4fd61279aca9f53a664e9e5f7e7e
- https://git.kernel.org/stable/c/1c8dc5b5517546c68ffae40b948336122bb61306
- https://git.kernel.org/stable/c/4f9ae386861e280b7631ca252f798d25575627ee
- https://git.kernel.org/stable/c/73ec7c96601d61d52310c659145bb06d933a0fa6
- https://git.kernel.org/stable/c/76149d53502cf17ef3ae454ff384551236fba867

- https://git.kernel.org/stable/c/c93a33f28f915d446eea6fb3f0e1def0b3af1982
- https://git.kernel.org/stable/c/dd8b13cb4ff1a4545a214ed897fdf2bc341155b6
- https://git.kernel.org/stable/c/fefa0fcd78be465b7ad4c497fa6ec90d64194c04
- https://github.com/torvalds/linux/commit/dd8b13cb4ff1a4545a214ed897fdf2bc341155b6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46259
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11805

7

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46270
BDU:2026-11809

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 4.2 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

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://nvd.nist.gov/vuln/detail/CVE-2026-46270
- https://security-tracker.debian.org/tracker/CVE-2026-46270
- https://git.kernel.org/linus/e2febe375e5ea5afed92f4cd9711bde8f24ee6d2
- https://git.kernel.org/stable/c/2178dc65d45e2f7bcaa8af8d80d100419bdab251
- https://git.kernel.org/stable/c/62d753b916bd500bb269b7078cdab73198ab4718
- https://git.kernel.org/stable/c/64e15155095f39f4dec9b4659da1238ef8fc54d4
- https://git.kernel.org/stable/c/721449a15170fc5f028a7576d7f65b9f60d53482
- https://git.kernel.org/stable/c/a39f8f06216f73ef40e71e2fe4ad071964c1fd36

- https://git.kernel.org/stable/c/af261f218a7606f93d2c786353d60bb4feb56ef0
- https://git.kernel.org/stable/c/d4e2e3c3caa26b93aa9f36d0a6824b584e2a8dfc
- https://git.kernel.org/stable/c/e2febe375e5ea5afed92f4cd9711bde8f24ee6d2
- https://github.com/torvalds/linux/commit/721449a15170fc5f028a7576d7f65b9f60d53482
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46270
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11809

8

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46267
BDU:2026-11808

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.7 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46267
- https://security-tracker.debian.org/tracker/CVE-2026-46267
- https://git.kernel.org/linus/c9efde1e537baed7648a94022b43836a348a074f
- https://git.kernel.org/stable/c/1cb97b1225450af3f7b728777929ba50c6a58ced
- https://git.kernel.org/stable/c/276820278e9717cc7d4bb32381892dd3ddf418d4
- https://git.kernel.org/stable/c/77eef9f2eef045c3c37a3df82d3e661afb866b98
- https://git.kernel.org/stable/c/a24a676329d40481b2331bfa1418a679577dfd3a
- https://git.kernel.org/stable/c/c60f41022eaad2a1dafecd3ae6f249a3bd6d4b6e

- https://git.kernel.org/stable/c/c9efde1e537baed7648a94022b43836a348a074f
- https://git.kernel.org/stable/c/cf70cedce327833296ebe6043364d1e44b76a2ab
- https://github.com/torvalds/linux/commit/1cb97b1225450af3f7b728777929ba50c6a58ced
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46267
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11808

9

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46265
BDU:2026-11807

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 5.7 до 6.1.165
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://nvd.nist.gov/vuln/detail/CVE-2026-46265
- https://security-tracker.debian.org/tracker/CVE-2026-46265
- https://git.kernel.org/linus/c0a26bbd3f99b7b03f072e3409aff4e6ec8af6f6
- https://git.kernel.org/stable/c/0cbec8b49270f3f0600b8e3ef5e8f0d233dcea27
- https://git.kernel.org/stable/c/12761bd0ae16a80f237c2a65ab1b1064076cc74a
- https://git.kernel.org/stable/c/562c96b1393da2df3ea62173c84117b39da353b9
- https://git.kernel.org/stable/c/70a5eb757ace5bd627a36f04d871eaf85def424d
- https://git.kernel.org/stable/c/c0a26bbd3f99b7b03f072e3409aff4e6ec8af6f6

- https://git.kernel.org/stable/c/c5ef9a1bcf5b597695d9c2e6ac452e9f89521862
- https://github.com/torvalds/linux/commit/c5ef9a1bcf5b597695d9c2e6ac452e9f89521862
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46265
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11807

10

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46253
BDU:2026-11804

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 3.5 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46253
- https://security-tracker.debian.org/tracker/CVE-2026-46253
- https://git.kernel.org/linus/5669645c052f235726a85f443769b6fc02f66762
- https://git.kernel.org/stable/c/06d2c8bd108cea503f6f6e13e47495ed1085275f
- https://git.kernel.org/stable/c/2fa9a047c6a50ec80c3890dd623b85e237f0d1fd
- https://git.kernel.org/stable/c/4f73486ca822305c1cf5b8ebc0b53a6ab3801a81
- https://git.kernel.org/stable/c/5669645c052f235726a85f443769b6fc02f66762
- https://git.kernel.org/stable/c/58bda5a1d1ee98254383ef34f76b2c35140513ea

- https://git.kernel.org/stable/c/7cfe964e61c0ab667abd5f5b68e0acbf783efa4f
- https://git.kernel.org/stable/c/9a6fc69a570c0780834246d52c856cc3dbc2605f
- https://git.kernel.org/stable/c/cff0ef043e16feb5a02307c8f9d0117a96c5587c
- https://github.com/torvalds/linux/commit/7cfe964e61c0ab667abd5f5b68e0acbf783efa4f
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46253
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11804

11

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23148
BDU:2026-11829

Идентификатор программной ошибки: CWE-696 Некорректный порядок работы

Уязвимый продукт: Linux: от 6.15.6 до 6.18.8 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://git.kernel.org/stable/c/68207ceefd71cc74ce4e983fa9bd10c3122e349b
- https://git.kernel.org/stable/c/ee10b06980acca1d46e0fa36d6fb4a9578eab6e4
- https://www.cve.org/CVERecord?id=CVE-2026-23148
- https://git.kernel.org/linus/0fcee2cfc4b2e16e62ff8e0cc2cd8dd24efad65e
- https://security-tracker.debian.org/tracker/CVE-2026-23148
- https://access.redhat.com/security/cve/CVE-2026-23148
- https://ubuntu.com/security/CVE-2026-23148

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11829

12

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46323
BDU:2026-11810

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.19 до 7.0.11
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46323
- https://security-tracker.debian.org/tracker/CVE-2026-46323
- https://gist.github.com/lcfr-eth/2566a5cef312c94a5ff8d62fa417955f
- https://git.kernel.org/linus/4db79a322db8c97f7b73b8a347395ef4d685eb40
- https://git.kernel.org/stable/c/1f9c828556416fbe3f49386708ce999fc4d4da06
- https://git.kernel.org/stable/c/44bea2032af0425e4ce6d26a8af0ede79db49ec1
- https://git.kernel.org/stable/c/479084ae0e1d9cb7929cb4298d35623de189f80a
- https://git.kernel.org/stable/c/4db79a322db8c97f7b73b8a347395ef4d685eb40

- https://git.kernel.org/stable/c/e334cbf3388fd9334503a778a82d9e9f14dd2f71
- https://lore.kernel.org/linux-cve-announce/2026060926-CVE-2026-46323-6830@gregkh/T/#u
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46323
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11810

13

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23158
BDU:2026-11830

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.11 до 6.12.68 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://git.kernel.org/stable/c/7bec90f605cfb138006f5ba575f2310593347110
- https://git.kernel.org/stable/c/815a8e3bf72811d402b30bd4a53cde5e9df7a563
- https://www.cve.org/CVERecord?id=CVE-2026-23158
- https://git.kernel.org/linus/53ad4a948a4586359b841d607c08fb16c5503230
- https://security-tracker.debian.org/tracker/CVE-2026-23158
- https://ubuntu.com/security/CVE-2026-23158
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11830

14

Краткое описание: Отказ в обслуживании в Apache ActiveMQ

Идентификатор уязвимости: CVE-2026-39304
BDU:2026-11865

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

Уязвимый продукт: Apache ActiveMQ Broker: от 6.0.0 до 6.2.4
Apache ActiveMQ All: от 6.0.0 до 6.2.4
Apache ActiveMQ: от 6.0.0 до 6.2.4
Apache ActiveMQ Client: от 6.0.0 до 6.2.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://activemq.apache.org/security-advisories.data/CVE-2026-39304-announcement.txt
- https://bdu.fstec.ru/vul/2026-11865

15

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23223
BDU:2026-11836

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.13 до 6.18.10 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://git.kernel.org/stable/c/1d411278dda293a507cb794db7d9ed3511c685c6
- https://git.kernel.org/stable/c/ed82e7949f5cac3058f4100f3cd670531d41a266
- https://git.kernel.org/stable/c/ba5264610423d9653aa36920520902d83841bcfd
- https://git.kernel.org/stable/c/1c253e11225bc5167217897885b85093e17c2217
- https://www.cve.org/CVERecord?id=CVE-2026-23223
- https://security-tracker.debian.org/tracker/CVE-2026-23223
- https://access.redhat.com/security/cve/CVE-2026-23223
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48

- https://bdu.fstec.ru/vul/2026-11836

16

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23233
BDU:2026-11837

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.9 до 6.12.73 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23233
- https://git.kernel.org/stable/c/d4534a7f6c92baaf7e12a45fc6e37332cafafc33
- https://git.kernel.org/stable/c/1ff415eef513bf12deb058fc50d57788c46c48e6
- https://git.kernel.org/stable/c/fee27b69dde1a05908b350eea42937af2387c4fe
- https://git.kernel.org/stable/c/607cb9d83838d2cd9f0406c2403ed61aadf0edff
- https://git.kernel.org/linus/5c145c03188bc9ba1c29e0bc4d527a5978fc47f9
- https://security-tracker.debian.org/tracker/CVE-2026-23233
- https://ubuntu.com/security/CVE-2026-23233

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11837

17

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23344
BDU:2026-11846

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 6.19.6 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23344
- https://git.kernel.org/stable/c/79a26fe3175b9ed7c0c9541b197cb9786237c0f7
- https://git.kernel.org/linus/889b0e2721e793eb46cf7d17b965aa3252af3ec8
- https://security-tracker.debian.org/tracker/CVE-2026-23344
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11846

18

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23387
BDU:2026-11850

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

Уязвимый продукт: Linux: от 6.17.10 до 6.18.16 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/stable/c/95b14ecc56881dd9a187e1e84dd0daa88ff22c5d
- https://git.kernel.org/stable/c/188ba3468cb7c098c62609d82e9fc58d29ead7f4
- https://git.kernel.org/stable/c/ea07fcfbba4301839db3784f09955d9fa3e98090
- https://git.kernel.org/stable/c/1e0465139fd9caee7ffefe285ef7d5f21919e474
- https://git.kernel.org/linus/fd5bed798f45eb3a178ad527b43ab92705faaf8a
- https://security-tracker.debian.org/tracker/CVE-2026-23387
- https://ubuntu.com/security/CVE-2026-23387
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48

- https://bdu.fstec.ru/vul/2026-11850

19

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23390
BDU:2026-11851

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 6.12 до 6.12.73 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23390
- https://git.kernel.org/stable/c/02d209bb018a40dee9eac89e91860253dee9605b
- https://git.kernel.org/stable/c/f2584f791a10343bdc995ff6ff402db45b95de69
- https://git.kernel.org/linus/daafcc0ef0b358d9d622b6e3b7c43767aa3814ee
- https://security-tracker.debian.org/tracker/CVE-2026-23390
- https://ubuntu.com/security/CVE-2026-23390
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11851

20

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-64907
BDU:2026-11853

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.112.26081010
Microsoft Office LTSC 2024: до 16.112.26081010
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5565.1000
Microsoft Office 365: до 16.112.26081010

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64907
- https://bdu.fstec.ru/vul/2026-11853

21

Краткое описание: Отказ в обслуживании в Apache Tomcat

Идентификатор уязвимости: CVE-2026-53434
BDU:2026-11857

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

Уязвимый продукт: Tomcat: от 9.0.0.M1 до 9.0.118 включительно

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://lists.apache.org/thread/x510lbq0sfrd1qyo7q3r1mpllgpdcosk
- https://bdu.fstec.ru/vul/2026-11857

22

Краткое описание: Получение конфиденциальной информации в Apache Tomcat

Идентификатор уязвимости: CVE-2026-55276
BDU:2026-11858

Идентификатор программной ошибки: CWE-670 Некорректная реализация хода выполнения команд

Уязвимый продукт: Tomcat: от 9.0.0.M1 до 9.0.118 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://lists.apache.org/thread/jy09xjlzn6r2qwvqoph8vcmf959yq68v
- https://bdu.fstec.ru/vul/2026-11858

23

Краткое описание: Обход безопасности в Apache Tomcat

Идентификатор уязвимости: CVE-2026-29129
BDU:2026-11862

Идентификатор программной ошибки: CWE-327 Использование скомпрометированного или ненадежного криптографического алгоритма

Уязвимый продукт: Tomcat: от 11.0.16 до 11.0.18 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://lists.apache.org/thread/r4h1t6f8xhxsxfm6c2z5cprolsosho3f
- https://bdu.fstec.ru/vul/2026-11862

24

Краткое описание: Выполнение произвольного кода в Apache ActiveMQ

Идентификатор уязвимости: CVE-2026-40466
BDU:2026-11864

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

Уязвимый продукт: Apache ActiveMQ Broker: от 6.0.0 до 6.2.3
Apache ActiveMQ: от 6.0.0 до 6.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt
- https://bdu.fstec.ru/vul/2026-11864

25

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46251
BDU:2026-11803

Идентификатор программной ошибки: CWE-237 Некорректная обработка структурных элементов

Уязвимый продукт: Linux: от 6.0.19 до 6.1.165
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

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://nvd.nist.gov/vuln/detail/CVE-2026-46251
- https://security-tracker.debian.org/tracker/CVE-2026-46251
- https://git.kernel.org/linus/3a1f4264daed4b419c325a7fe35e756cada3cf82
- https://git.kernel.org/stable/c/201091da34c4f113af6b4a7407091c39bf29d4ca
- https://git.kernel.org/stable/c/3a1f4264daed4b419c325a7fe35e756cada3cf82
- https://git.kernel.org/stable/c/4eb830847d84276f1c8ea46541cfeeedaba1fb63
- https://git.kernel.org/stable/c/6e10283b5519d987d880d71bec90cdc7f2ec62b3
- https://git.kernel.org/stable/c/80e1fda9c084dcf54819a12bc7682ec0afd2d8f4

- https://git.kernel.org/stable/c/e3d1fd084319f8f0830b22f014c7af6a96b4497b
- https://github.com/torvalds/linux/commit/201091da34c4f113af6b4a7407091c39bf29d4ca
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-46251
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11803

26

Краткое описание: Отказ в обслуживании в Apache Neethi

Идентификатор уязвимости: CVE-2026-42403
BDU:2026-11868

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

Уязвимый продукт: Apache Neethi: до 3.2.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://lists.apache.org/thread/zm6t8skkkskjwk1881l4m4n0l7dqclzo
- https://bdu.fstec.ru/vul/2026-11868

27

Краткое описание: Отказ в обслуживании в Apache Neethi

Идентификатор уязвимости: CVE-2026-42402
BDU:2026-11869

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

Уязвимый продукт: Apache Neethi: до 3.2.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-14 / 2026-08-14

Ссылки на источник:

- https://lists.apache.org/thread/p826j0phhmr9f83wzpmys1y0bdfrr2q4
- https://bdu.fstec.ru/vul/2026-11869

28

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23200
BDU:2026-11834

Идентификатор программной ошибки: CWE-1027 Топ-10 OWASP — 2017 Категория A1 - Внедрение

Уязвимый продукт: Linux: от 6.18.2 до 6.18.9 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/stable/c/d8143c54ceeba232dc8a13aa0afa14a44b371d93
- https://git.kernel.org/stable/c/50b7c7a255858a85c4636a1e990ca04591153dca
- https://git.kernel.org/stable/c/b8ad2d53f706aeea833d23d45c0758398fede580
- https://www.cve.org/CVERecord?id=CVE-2026-23200
- https://git.kernel.org/linus/bbf4a17ad9ffc4e3d7ec13d73ecd59dea149ed25
- https://security-tracker.debian.org/tracker/CVE-2026-23200
- https://access.redhat.com/security/cve/CVE-2026-23200

- https://ubuntu.com/security/CVE-2026-23200
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11834

29

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45984
BDU:2026-11799

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 5.2 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45984
- https://security-tracker.debian.org/tracker/CVE-2026-45984
- https://git.kernel.org/linus/faddeb848305e79db89ee0479bb0e33380656321
- https://git.kernel.org/stable/c/1403989d1b502f4a2c0d0b42ccf1c25748442eff
- https://git.kernel.org/stable/c/1cae1bafdf9caa9b462b19af06b1a06902e4e142
- https://git.kernel.org/stable/c/6d76febba07c40bcf358f63216d36ea68cf1c215
- https://git.kernel.org/stable/c/764c3c84b5683e608f43735c803a5f415046686c
- https://git.kernel.org/stable/c/815ddd27c0c7171a99fe802fdb19098ddef8b19d

- https://git.kernel.org/stable/c/87d4954b5c59735a99ea98cb208d47130f6dce7d
- https://git.kernel.org/stable/c/d87268326b277af3665237ac76a73dd9fa8e21b4
- https://git.kernel.org/stable/c/faddeb848305e79db89ee0479bb0e33380656321
- https://github.com/torvalds/linux/commit/815ddd27c0c7171a99fe802fdb19098ddef8b19d
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45984
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11799

30

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43278
BDU:2026-11734

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 4.14 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43278
- https://security-tracker.debian.org/tracker/CVE-2026-43278
- https://git.kernel.org/linus/fb8a6c18fb9a6561f7a15b58b272442b77a242dd
- https://git.kernel.org/stable/c/3d746b639be4b4f5cd8ce2b06aa52dc443f50edc
- https://git.kernel.org/stable/c/7daf279c674d515fb22a727a7bbc92aeb35c5442
- https://git.kernel.org/stable/c/83d72091804600ead96dc9e9f518ea56cb4942f6
- https://git.kernel.org/stable/c/8d9ddad561136f7e6a9346767bf97b4d79e38e67
- https://git.kernel.org/stable/c/9a95b98202113045bc1a5bcb30388a500f25e050

- https://git.kernel.org/stable/c/b1c1a2637ebd675aa2d71fee8c70da8791d73850
- https://git.kernel.org/stable/c/e2e738e8dfbbf83bd2bae0467ec4420cc52da42a
- https://git.kernel.org/stable/c/fb8a6c18fb9a6561f7a15b58b272442b77a242dd
- https://github.com/torvalds/linux/commit/83d72091804600ead96dc9e9f518ea56cb4942f6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43278
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11734

31

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45970
BDU:2026-11792

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.0 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45970
- https://security-tracker.debian.org/tracker/CVE-2026-45970
- https://git.kernel.org/linus/e6834a4c474697df23ab9948fd3577b26bf48656
- https://git.kernel.org/stable/c/c65cdf46ce340c9c00fbbaf84599d2daff43626e
- https://git.kernel.org/stable/c/d31065526f160ee0244a719230aa069daca2bf4d
- https://git.kernel.org/stable/c/db5435b5342e3aaa4521d0f3ccfe94316b253ca1
- https://git.kernel.org/stable/c/de7c097800f07f3c108185c7a38b53a530ba30ff
- https://git.kernel.org/stable/c/e6834a4c474697df23ab9948fd3577b26bf48656

- https://git.kernel.org/stable/c/f94a0de7b9f32745a14a1621c63087a092823587
- https://git.kernel.org/stable/c/fd54ddc929be1d6c3b3b7b35d6d4642a5d9e803c
- https://git.kernel.org/stable/c/fef13c403be3fb685cb06419e6b3623106aab5ba
- https://github.com/torvalds/linux/commit/d31065526f160ee0244a719230aa069daca2bf4d
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45970
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11792

32

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23230
BDU:2026-11663

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.1 до 6.1.164
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-23230
- https://security-tracker.debian.org/tracker/CVE-2026-23230
- https://git.kernel.org/linus/ec306600d5ba7148c9dbf8f5a8f1f5c1a044a241
- https://git.kernel.org/stable/c/3eaa22d688311c708b73f3c68bc6d0c8e3f0f77a
- https://git.kernel.org/stable/c/4386f6af8aaedd0c5ad6f659b40cadcc8f423828
- https://git.kernel.org/stable/c/4cfa4c37dcbcfd70866e856200ed8a2894cac578
- https://git.kernel.org/stable/c/569fecc56bfe4df66f05734d67daef887746656b
- https://git.kernel.org/stable/c/c4b9edd55987384a1f201d3d07ff71e448d79c1b

- https://git.kernel.org/stable/c/ec306600d5ba7148c9dbf8f5a8f1f5c1a044a241
- https://github.com/torvalds/linux/commit/4cfa4c37dcbcfd70866e856200ed8a2894cac578
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23230
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11663

33

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23242
BDU:2026-11664

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 5.3 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://nvd.nist.gov/vuln/detail/CVE-2026-23242
- https://security-tracker.debian.org/tracker/CVE-2026-23242
- https://git.kernel.org/linus/14ab3da122bd18920ad57428f6cf4fade8385142
- https://git.kernel.org/stable/c/14ab3da122bd18920ad57428f6cf4fade8385142
- https://git.kernel.org/stable/c/714c99e1dc8f85f446e05be02ba83972e981a817
- https://git.kernel.org/stable/c/8564dcc12fbb372d984ab45768cae9335777b274
- https://git.kernel.org/stable/c/87b7a036d2c73d5bb3ae2d47dee23de465db3355
- https://git.kernel.org/stable/c/ab61841633d10e56a58c1493a262f0d02dba2f5e

- https://git.kernel.org/stable/c/ab957056192d6bd068b3759cb2077d859cca01f0
- https://git.kernel.org/stable/c/ce025f7f5d070596194315eb2e4e89d568b8a755
- https://git.kernel.org/stable/c/ffba40b67663567481fa8a1ed5d2da36897c175d
- https://github.com/torvalds/linux/commit/ce025f7f5d070596194315eb2e4e89d568b8a755
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23242
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11664

34

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23243
BDU:2026-11665

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 2.6.24 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-23243
- https://security-tracker.debian.org/tracker/CVE-2026-23243
- https://git.kernel.org/linus/5551b02fdbfd85a325bb857f3a8f9c9f33397ed2
- https://git.kernel.org/stable/c/1371ef6b1ecf3676b8942f5dfb3634fb0648128e
- https://git.kernel.org/stable/c/205955f29c26330b1dc7fdeadd5bb97c38e26f56
- https://git.kernel.org/stable/c/362e45fd9069ffa1523f9f1633b606ebf72060d7
- https://git.kernel.org/stable/c/52ab82cc5cf8ada5c3fb6ffe8f32fdb2fc27a34b
- https://git.kernel.org/stable/c/5551b02fdbfd85a325bb857f3a8f9c9f33397ed2

- https://git.kernel.org/stable/c/6eb2919474ca105c5b13d19574e25f0ddcf19ca2
- https://git.kernel.org/stable/c/9c80d688f402539dfc8f336de1380d6b4ee14316
- https://git.kernel.org/stable/c/a6a3e4af10993cb9e4b8f0548680aba0ab5f3b0d
- https://github.com/torvalds/linux/commit/52ab82cc5cf8ada5c3fb6ffe8f32fdb2fc27a34b
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11665

35

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23268
BDU:2026-11667

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Linux: от 6.13 до 6.18.18
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-23268
- https://security-tracker.debian.org/tracker/CVE-2026-23268
- https://git.kernel.org/linus/6601e13e82841879406bf9f369032656f441a425
- https://git.kernel.org/stable/c/0fc63dd9170643d15c25681fca792539e23f4640
- https://git.kernel.org/stable/c/17debf5586020790b5717f96e5e6a3ca5bb961ab
- https://git.kernel.org/stable/c/33ee909702e047c94aaf41d4eea35626d509802c
- https://git.kernel.org/stable/c/4cafce4d6d0a66ec27e3af5637c11901d60189fa
- https://git.kernel.org/stable/c/6601e13e82841879406bf9f369032656f441a425

- https://git.kernel.org/stable/c/a407a078cd41b5261b99d822af784bd9f136eb4d
- https://git.kernel.org/stable/c/b60b3f7a35c46b2e0ca934f9c988b8fca06d76c6
- https://git.kernel.org/stable/c/b6a94eeca9c6c8f7c55ad44c62c98324f51ec596
- https://github.com/torvalds/linux/commit/b60b3f7a35c46b2e0ca934f9c988b8fca06d76c6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23268
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11667

36

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23272
BDU:2026-11669

Идентификатор программной ошибки: CWE-371 Уязвимости, связанные с состоянием

Уязвимый продукт: Linux: от 4.9.33 до 6.18.17
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-23272
- https://security-tracker.debian.org/tracker/CVE-2026-23272
- https://git.kernel.org/linus/def602e498a4f951da95c95b1b8ce8ae68aa733a
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=def602e498a4f951da95c95b1b8ce8ae68aa733a
- https://git.kernel.org/stable/c/6826131c7674329335ca25df2550163eb8a1fd0c
- https://git.kernel.org/stable/c/ccb8c8f3c1127cf34d18c737309897c68046bf21
- https://git.kernel.org/stable/c/def602e498a4f951da95c95b1b8ce8ae68aa733a
- https://github.com/AIS0127/security-research/tree/kernelctf-exp451/pocs/linux/kernelctf/CVE-2026-23272_cos

- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23272
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11669

37

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23273
BDU:2026-11670

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

Уязвимый продукт: Linux: от 6.18.10 до 6.18.14
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-23273
- https://security-tracker.debian.org/tracker/CVE-2026-23273
- https://git.kernel.org/linus/e3f000f0dee1bfab52e2e61ca6a3835d9e187e35
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e3f000f0dee1bfab52e2e61ca6a3835d9e187e35
- https://git.kernel.org/stable/c/19c7d8ac51988d053709c1e85bd8482076af845d
- https://git.kernel.org/stable/c/1e58ae87ad1e6e24368dea9aec9048c758cd0e2b
- https://git.kernel.org/stable/c/3d94323c80d7fc4da5f10f9bb06a45d39d5d3cc4
- https://git.kernel.org/stable/c/721eb342d9ba19bad5c4815ea3921465158b7362

- https://git.kernel.org/stable/c/91e4ff8d966978901630fc29582c1a76d3c6e46c
- https://git.kernel.org/stable/c/a1f686d273d129b45712d95f4095843b864466bd
- https://git.kernel.org/stable/c/d34f7a8aa9a25b7e64e0e46e444697c0f702374d
- https://git.kernel.org/stable/c/e3f000f0dee1bfab52e2e61ca6a3835d9e187e35
- https://github.com/4ab48b3f1ded2472/security-research/tree/CVE-2026-23273_cos/pocs/linux/kernelctf/CVE-2026-23273_cos
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23273
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11670

38

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43128
BDU:2026-11674

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 6.13 до 6.18.16
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43128
- https://security-tracker.debian.org/tracker/CVE-2026-43128
- https://git.kernel.org/linus/104016eb671e19709721c1b0048dd912dc2e96be
- https://git.kernel.org/stable/c/104016eb671e19709721c1b0048dd912dc2e96be
- https://git.kernel.org/stable/c/40126bcbefa79ea86672e05dae608596bab38319
- https://git.kernel.org/stable/c/70542b69abff34d24b11ae0bb200cc7a766d18df
- https://git.kernel.org/stable/c/b324327ff6f48d8065dca67eb3b91357e72726bd
- https://git.kernel.org/stable/c/ba3bf0f1bf1d5d0404678485e872980532fcc2c4

- https://git.kernel.org/stable/c/d3e32e2f3262f1b25d77c085ace38e2cc4ad75cf
- https://github.com/torvalds/linux/commit/40126bcbefa79ea86672e05dae608596bab38319
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43128
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11674

39

Краткое описание: Внедрение кода в Linux

Идентификатор уязвимости: CVE-2026-43134
BDU:2026-11677

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 3.14 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Внедрение кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43134
- https://security-tracker.debian.org/tracker/CVE-2026-43134
- https://git.kernel.org/linus/138d7eca445ef37a0333425d269ee59900ca1104
- https://git.kernel.org/stable/c/138d7eca445ef37a0333425d269ee59900ca1104
- https://git.kernel.org/stable/c/335071c0c3637064ec250481f589075db44fe4e6
- https://git.kernel.org/stable/c/481ea39b342c347b6ac029f3d418486280be4e45
- https://git.kernel.org/stable/c/8dd43f9a9323f9c01bc8246da8d81a4c783c9e97
- https://git.kernel.org/stable/c/9118601ff90b79e8df3c0c98f48ae00c1b02ecef

- https://git.kernel.org/stable/c/96581749c7c14fbec32c35728520867929600041
- https://git.kernel.org/stable/c/ec91078e132179b04e0c3906b599816c056ceaad
- https://git.kernel.org/stable/c/fa6ad76fa8623c0a50d529cd5726fa5d819a3be4
- https://github.com/torvalds/linux/commit/8dd43f9a9323f9c01bc8246da8d81a4c783c9e97
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43134
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11677

40

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43158
BDU:2026-11689

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.11 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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://nvd.nist.gov/vuln/detail/CVE-2026-43158
- https://security-tracker.debian.org/tracker/CVE-2026-43158
- https://git.kernel.org/linus/3eefc0c2b78444b64feeb3783c017d6adc3cd3ce
- https://git.kernel.org/stable/c/24ce71852f2cee6581e2cbebc15489ed52bf63b7
- https://git.kernel.org/stable/c/38613c01f69e1e77e6b8acab1e8ac665d01c2f15
- https://git.kernel.org/stable/c/3eefc0c2b78444b64feeb3783c017d6adc3cd3ce
- https://git.kernel.org/stable/c/43f3b18679615a93bd848afde3602ba160637a46
- https://git.kernel.org/stable/c/6a8737afbccc340e718e0b22577312826390be8b

- https://git.kernel.org/stable/c/a396b3d73d51355e50acdb403ba9c4cae4c1174e
- https://git.kernel.org/stable/c/d08976725355b9d54d8332fce223fa281cc304a5
- https://git.kernel.org/stable/c/ef42a8766ff3fdf51cf72fb36d0859c09d134478
- https://github.com/torvalds/linux/commit/24ce71852f2cee6581e2cbebc15489ed52bf63b7
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43158
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11689

41

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43180
BDU:2026-11695

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 5.11 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43180
- https://security-tracker.debian.org/tracker/CVE-2026-43180
- https://git.kernel.org/linus/64868f5ecadeb359a49bc4485bfa7c497047f13a
- https://git.kernel.org/stable/c/443a830b1dc4f85c7560da59d4494b629feee215
- https://git.kernel.org/stable/c/586318c2730433184c6f1d21183e346ddf25e81d
- https://git.kernel.org/stable/c/64868f5ecadeb359a49bc4485bfa7c497047f13a
- https://git.kernel.org/stable/c/8367c0e90126426e60581e4c07e1ec4411a0f843
- https://git.kernel.org/stable/c/9c79b839a63980c7da7ec5db895198045e154112

- https://git.kernel.org/stable/c/a2cd4b4db315a845a5603d08c9d03b11ddfc799d
- https://git.kernel.org/stable/c/ef9b10a020503888eb6c8ed85a3d901a624ede4c
- https://git.kernel.org/stable/c/fc393af769af845d9985e2845e49553d8f015a64
- https://github.com/torvalds/linux/commit/8367c0e90126426e60581e4c07e1ec4411a0f843
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43180
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11695

42

Краткое описание: Получение конфиденциальной информации в Linux

Идентификатор уязвимости: CVE-2026-43184
BDU:2026-11698

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 5.8 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

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://nvd.nist.gov/vuln/detail/CVE-2026-43184
- https://security-tracker.debian.org/tracker/CVE-2026-43184
- https://git.kernel.org/linus/69d26698e4fd44935510553809007151b2fe4db5
- https://git.kernel.org/stable/c/30868a6a5238849d554295aff3ce61d242d7fad8
- https://git.kernel.org/stable/c/69d26698e4fd44935510553809007151b2fe4db5
- https://git.kernel.org/stable/c/7aac0a30dcf41cdb510526740d9a2ab1520c5d98
- https://git.kernel.org/stable/c/852475278ca5e96e0c0275950e1a84203e602b33
- https://git.kernel.org/stable/c/b646e54d23b9b592d612a2036aab14e0f6c14206

- https://git.kernel.org/stable/c/c94ede3c436dfbd9cedd9cb69f604f6fc901b6a2
- https://git.kernel.org/stable/c/e2cacec7d4291300a282feb3af8eba57b93b15aa
- https://git.kernel.org/stable/c/e4272754063d52c9ad0169865add8816ba696471
- https://github.com/torvalds/linux/commit/852475278ca5e96e0c0275950e1a84203e602b33
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43184
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11698

43

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43187
BDU:2026-11699

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

Уязвимый продукт: Linux: от 5.11 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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://nvd.nist.gov/vuln/detail/CVE-2026-43187
- https://security-tracker.debian.org/tracker/CVE-2026-43187
- https://git.kernel.org/linus/6f13c1d2a6271c2e73226864a0e83de2770b6f34
- https://git.kernel.org/stable/c/479b05fc3ee272090f671b06a41f3da8aa78eece
- https://git.kernel.org/stable/c/6f13c1d2a6271c2e73226864a0e83de2770b6f34
- https://git.kernel.org/stable/c/a631899025d47ea1aa6464d76db5b4d3b6d196fd
- https://git.kernel.org/stable/c/aa9083d97e2157da3c6fb45ddb1a97af7f188f7f
- https://git.kernel.org/stable/c/e1b8c6452ee99a30e188a88f3f3f804fb1c6004a

- https://git.kernel.org/stable/c/f31a8334e1c54b126fcecf98645a49b6bc5ad399
- https://git.kernel.org/stable/c/f3c0d1fc1eadbb4adbee5ab7757d41d35f48325b
- https://git.kernel.org/stable/c/ffaf5c99d0f862db021fb1af8b813c1416b1beb2
- https://github.com/torvalds/linux/commit/479b05fc3ee272090f671b06a41f3da8aa78eece
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43187
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11699

44

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43205
BDU:2026-11702

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.13 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43205
- https://security-tracker.debian.org/tracker/CVE-2026-43205
- https://git.kernel.org/linus/8a5752c6dcc085a3bfc78589925182e4e98468c5
- https://git.kernel.org/stable/c/89764cf44544e943230f5e03b8c40a90da26537c
- https://git.kernel.org/stable/c/8a5752c6dcc085a3bfc78589925182e4e98468c5
- https://git.kernel.org/stable/c/8b841fd529db9faf8bc678d429d4bf4e98b10900
- https://git.kernel.org/stable/c/a26dda3bae469c8e4e1b1993ad33dafa32d0fc28
- https://git.kernel.org/stable/c/a3034a8d56174dd6464c46823438f25797910a8d

- https://git.kernel.org/stable/c/b690635d4719214892855b79ce018d4b1672ac96
- https://git.kernel.org/stable/c/c18493f750208eb4ff1198fc5a02786b8b2d70a6
- https://github.com/torvalds/linux/commit/c18493f750208eb4ff1198fc5a02786b8b2d70a6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43205
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11702

45

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43212
BDU:2026-11704

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 5.19 до 6.1.165
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43212
- https://security-tracker.debian.org/tracker/CVE-2026-43212
- https://git.kernel.org/linus/94b0c831eda778ae9e4f2164a8b3de485d8977bb
- https://git.kernel.org/stable/c/1d8f2f024801019d85159a020b72a4424b46bcf4
- https://git.kernel.org/stable/c/61a56df2fbaad3a4d00f0c6a904b5d1ee8982eb4
- https://git.kernel.org/stable/c/92adfb707beec0fe956424373654a70aad35ea13
- https://git.kernel.org/stable/c/94b0c831eda778ae9e4f2164a8b3de485d8977bb
- https://git.kernel.org/stable/c/b5bf05e05cdf489a04137e4da407de9d4cca5295

- https://git.kernel.org/stable/c/bb1a54f7f011f19ed936632698eae574e0b91063
- https://github.com/torvalds/linux/commit/1d8f2f024801019d85159a020b72a4424b46bcf4
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43212
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11704

46

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43226
BDU:2026-11709

Идентификатор программной ошибки: CWE-372 Некорректное определение внутреннего состояния

Уязвимый продукт: Linux: от 4.8 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://nvd.nist.gov/vuln/detail/CVE-2026-43226
- https://security-tracker.debian.org/tracker/CVE-2026-43226
- https://git.kernel.org/linus/ad22d24be635c6beab6a1fdd3f8b1f3c478d15da
- https://git.kernel.org/stable/c/19e384a7d00d888303a8285977cdf1970c6cccd6
- https://git.kernel.org/stable/c/81248b1eb3c5954cc1fc7b33b7c03e34d20cb8c8
- https://git.kernel.org/stable/c/899ef00963ce76f9fc421a7d02335fe4ead6389b
- https://git.kernel.org/stable/c/9bcd7c00691a2db9745817d5ea79262a503b135c
- https://git.kernel.org/stable/c/9ff599a9be784a808c36765086e3db2144aa3b66

- https://git.kernel.org/stable/c/a179ac7be8f5a650d0068040705f4cddd6ca369c
- https://git.kernel.org/stable/c/ad22d24be635c6beab6a1fdd3f8b1f3c478d15da
- https://git.kernel.org/stable/c/f0f729bdffb08af32e0f54521b81b8a9e0321f16
- https://github.com/torvalds/linux/commit/9ff599a9be784a808c36765086e3db2144aa3b66
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43226
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11709

47

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-68138
BDU:2026-11717

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

Уязвимый продукт: Linux: до 7.2 rc5
Red Hat Enterprise Linux: 9
Ubuntu: 26.04 LTS
Red Hat Enterprise Linux for NVIDIA: 26

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/aramosf/CVE-2026-68138
- https://git.kernel.org/stable/c/f43ee0c0730d6191629b5ee1ceae27b1ebfdc047
- https://git.kernel.org/stable/c/fb29e1b41052488ee3f2d115d4a870497ebd7f7d
- https://access.redhat.com/security/cve/cve-2026-68138
- https://ubuntu.com/security/CVE-2026-68138
- https://bdu.fstec.ru/vul/2026-11717

48

Краткое описание: Получение конфиденциальной информации в GitPython

Идентификатор уязвимости: CVE-2026-73620
BDU:2026-11719

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

Уязвимый продукт: GitPython: до 3.1.56 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-3f7w-8rr8-f37f
- https://www.vulncheck.com/advisories/gitpython-before-arbitrary-file-overwrite-and-read
- https://bdu.fstec.ru/vul/2026-11719

49

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-73623
BDU:2026-11720

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

Уязвимый продукт: GitPython: до 3.1.53 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-6p8h-3wgx-97gf
- https://www.vulncheck.com/advisories/gitpython-before-remote-code-execution-via-template
- https://bdu.fstec.ru/vul/2026-11720

50

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43279
BDU:2026-11735

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 3.5 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43279
- https://security-tracker.debian.org/tracker/CVE-2026-43279
- https://git.kernel.org/linus/fba2105a157fffcf19825e4eea498346738c9948
- https://git.kernel.org/stable/c/6af16f1b8649df4c00d6ced924bdd8b72c885b6a
- https://git.kernel.org/stable/c/780dc57794a217b49994fa1d0b42465fb10a00aa
- https://git.kernel.org/stable/c/8995fc0e00b3fee9bf7ecb3d836b635b730c1049
- https://git.kernel.org/stable/c/ccaf9296763be4f76b59e2cac377006016c34435
- https://git.kernel.org/stable/c/fa01973bb79d70c4736b6a4b2de99fbb2cbc8d1f

- https://git.kernel.org/stable/c/fba2105a157fffcf19825e4eea498346738c9948
- https://git.kernel.org/stable/c/fc9e5af60dc199051dc202ae78e1fe76a9977a5e
- https://github.com/torvalds/linux/commit/ccaf9296763be4f76b59e2cac377006016c34435
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43279
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11735

51

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43283
BDU:2026-11736

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

Уязвимый продукт: Linux: от 3.15 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43283
- https://security-tracker.debian.org/tracker/CVE-2026-43283
- https://git.kernel.org/linus/ffe68c3766997d82e9ccaf1cdbd47eba269c4aa2
- https://git.kernel.org/stable/c/0f589ee54fd6d76d3f75e745f7f12c64cbd749e5
- https://git.kernel.org/stable/c/1b1371cd4032ae859838ebc74215f569987bb197
- https://git.kernel.org/stable/c/1b1d3c5d58a80a19d017a409aa2308162bab5bbf
- https://git.kernel.org/stable/c/1e300c33ef3cc544c2b9c693778fe9490cfe9184

- https://git.kernel.org/stable/c/7e54ff938bebb173822b4c38b33fc164c1cabf92
- https://git.kernel.org/stable/c/8320727be7ff704e07c87624efc2a4a75f54b3ce
- https://git.kernel.org/stable/c/accd0599bc8e73b962247c6c6c70ca7aa1f8e8d0
- https://git.kernel.org/stable/c/ffe68c3766997d82e9ccaf1cdbd47eba269c4aa2
- https://github.com/torvalds/linux/commit/7e54ff938bebb173822b4c38b33fc164c1cabf92
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43283
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11736

52

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43291
BDU:2026-11738

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 6.17.3 до 6.18.16
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-43291
- https://security-tracker.debian.org/tracker/CVE-2026-43291
- https://git.kernel.org/linus/571dcbeb8e635182bb825ae758399831805693c2
- https://git.kernel.org/stable/c/3b91160e9a91b5a2662875417dc42dc5b0bf03ea
- https://git.kernel.org/stable/c/498fc5d0d650c77e87fcc73808d4f43240c21805
- https://git.kernel.org/stable/c/571dcbeb8e635182bb825ae758399831805693c2
- https://git.kernel.org/stable/c/a24a8a582da4426b2042e510a1080df84083b51d
- https://git.kernel.org/stable/c/ad058a4317db7fdb3f09caa6ed536d24a62ce6a0

- https://git.kernel.org/stable/c/c692db813a7e3b7c3c17d6e9a3ad2a018bf1142b
- https://git.kernel.org/stable/c/f5218426f765eee22e178df9c126d974792fb6a5
- https://github.com/torvalds/linux/commit/498fc5d0d650c77e87fcc73808d4f43240c21805
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43291
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11738

53

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43296
BDU:2026-11740

Идентификатор программной ошибки: CWE-667 Некорректная блокировка

Уязвимый продукт: Linux: от 5.5 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://nvd.nist.gov/vuln/detail/CVE-2026-43296
- https://security-tracker.debian.org/tracker/CVE-2026-43296
- https://git.kernel.org/linus/70e9a5760abfb6338d63994d4de6b0778ec795d6
- https://git.kernel.org/stable/c/36cc5a5e0178d5fb79e04173b8aa623b0108819a
- https://git.kernel.org/stable/c/70e9a5760abfb6338d63994d4de6b0778ec795d6
- https://git.kernel.org/stable/c/8052d0587fb14b85539c3a14a226586c0c3d6b4c
- https://git.kernel.org/stable/c/9a3fd301329474f449e75f86d8a4f6b9c603fd6c
- https://git.kernel.org/stable/c/b7eba260a34e854e2487b8363c11976f082df00d

- https://git.kernel.org/stable/c/cec2ceb35ce7bc874c43812bb39200d6cf691b87
- https://git.kernel.org/stable/c/d0b3c8a80336029d9356f429151eb27922d80a3c
- https://git.kernel.org/stable/c/d9b549b6951ba178ec14339a031cae65f4e43fe1
- https://github.com/torvalds/linux/commit/b7eba260a34e854e2487b8363c11976f082df00d
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-43296
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11740

54

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45852
BDU:2026-11748

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 4.19.86 до 5.10.252
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45852
- https://security-tracker.debian.org/tracker/CVE-2026-45852
- https://git.kernel.org/linus/0beefd0e15d962f497aad750b2d5e9c3570b66d1
- https://git.kernel.org/stable/c/0beefd0e15d962f497aad750b2d5e9c3570b66d1
- https://git.kernel.org/stable/c/22b8c23a3b92d023614bb00896fe364b2c1a31d3
- https://git.kernel.org/stable/c/26793db60925df1e88a29466813d586cbc190b8c
- https://git.kernel.org/stable/c/26a9cfe12f4ffdeaa136f252478986fa5f397ddc
- https://git.kernel.org/stable/c/5c07aef09a121a4cd622a71eb0753a9e135c84a8

- https://git.kernel.org/stable/c/af5956243018918130d52c9f671efdb40bab3366
- https://git.kernel.org/stable/c/ce6f8e007682f378279d4cf83b240f12d52c723b
- https://git.kernel.org/stable/c/d286f0d4e3ad3caf5f0e673cdad7bf89bf37d947
- https://github.com/torvalds/linux/commit/26a9cfe12f4ffdeaa136f252478986fa5f397ddc
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45852
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11748

55

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45860
BDU:2026-11751

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

Уязвимый продукт: Linux: от 5.15.198 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45860
- https://security-tracker.debian.org/tracker/CVE-2026-45860
- https://git.kernel.org/linus/21d033e472735ecec677f1ae46d6740b5e47a4f3
- https://git.kernel.org/stable/c/0792ad077d776c2dcf20f0484e2461ded1b77a24
- https://git.kernel.org/stable/c/0af0812baf2d363176c9b76fc07e33f13aede8db
- https://git.kernel.org/stable/c/13eede458fdf231f1bf96a398feea4ad1553f14c
- https://git.kernel.org/stable/c/21d033e472735ecec677f1ae46d6740b5e47a4f3
- https://git.kernel.org/stable/c/3d0994ed0aa1fc0a2c5e620b765e8defdd021bff

- https://git.kernel.org/stable/c/6e5fa7add3e76da068a478d905be64be8fa4e80a
- https://git.kernel.org/stable/c/a5c9e14e0e8923218ae881d5e78c990c07694966
- https://git.kernel.org/stable/c/fa85432d58c8e74b39333edbf8d28df2985dfc79
- https://github.com/torvalds/linux/commit/0af0812baf2d363176c9b76fc07e33f13aede8db
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45860
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11751

56

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45862
BDU:2026-11752

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 6.2.3 до 6.6.128
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45862
- https://security-tracker.debian.org/tracker/CVE-2026-45862
- https://git.kernel.org/linus/22d169bdd2849fe6bd18c2643742e1c02be6451c
- https://git.kernel.org/stable/c/0616137b70e6d9a547d4b60df8e1b64e36d83661
- https://git.kernel.org/stable/c/22d169bdd2849fe6bd18c2643742e1c02be6451c
- https://git.kernel.org/stable/c/36244dfd3853f7bf89d03b8e90d56b23ce7fbc16
- https://git.kernel.org/stable/c/36990407cdd257473607e33802d00e978af2759e
- https://git.kernel.org/stable/c/5962c30a6f05ea1ab73f039e235bb30716243517

- https://git.kernel.org/stable/c/c93f23375d8c410954b0df825e814b632fd62b9d
- https://git.kernel.org/stable/c/cd75e77125c8a51754ca4cd60b4ca083ed735d1d
- https://git.kernel.org/stable/c/d15cda135148ea7ba929cfdbcf208182bc29a7aa
- https://github.com/torvalds/linux/commit/d15cda135148ea7ba929cfdbcf208182bc29a7aa
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45862
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11752

57

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45935
BDU:2026-11780

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

Уязвимый продукт: Linux: от 6.7 до 6.12.75
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45935
- https://security-tracker.debian.org/tracker/CVE-2026-45935
- https://git.kernel.org/linus/b2bc7c44ed1779fc9eaab9a186db0f0d01439622
- https://git.kernel.org/stable/c/36c03f7f177b34d51f1cf1d2304b1074607bf4b0
- https://git.kernel.org/stable/c/78942172d5bff4d4afed8674abc09cc560ce44a0
- https://git.kernel.org/stable/c/a584b9d1059b29e97e17c919274e9adfb846f2a0
- https://git.kernel.org/stable/c/b271c9cb85927210b1b799e55ee7f702d12b4336
- https://git.kernel.org/stable/c/b2bc7c44ed1779fc9eaab9a186db0f0d01439622

- https://git.kernel.org/stable/c/c065541b71b79874c83d418a9acd18ad5826339b
- https://git.kernel.org/stable/c/f3b437a4c3e022a1449658ae9f3dd34859894513
- https://github.com/torvalds/linux/commit/f3b437a4c3e022a1449658ae9f3dd34859894513
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45935
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11780

58

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45946
BDU:2026-11783

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 5.13.4 до 5.15.202
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-45946
- https://security-tracker.debian.org/tracker/CVE-2026-45946
- https://git.kernel.org/linus/c4af8a98bb52825a5331ae1d0604c0ea6956ba4b
- https://git.kernel.org/stable/c/43cbb78ee047b9b12d096d40e3be265969d4c1f8
- https://git.kernel.org/stable/c/46dbda27b028d78087667e8280966b99cec015ca
- https://git.kernel.org/stable/c/551672981fe227122258a25a385a05f5c0746ad6
- https://git.kernel.org/stable/c/709db4b476e254579d9c48ec34d397a41ca0c407
- https://git.kernel.org/stable/c/847eeb6c0efcd76c7def73857cf798a4fcd8f79b

- https://git.kernel.org/stable/c/c4af8a98bb52825a5331ae1d0604c0ea6956ba4b
- https://git.kernel.org/stable/c/f50433f2603def08b21a4bf2fd238687fb5cbde9
- https://github.com/torvalds/linux/commit/46dbda27b028d78087667e8280966b99cec015ca
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45946
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11783

59

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-45972
BDU:2026-11793

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.18.10 до 6.18.14
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://nvd.nist.gov/vuln/detail/CVE-2026-45972
- https://security-tracker.debian.org/tracker/CVE-2026-45972
- https://git.kernel.org/linus/ebbbc4bfad4cb355d17c671223d0814ee3ef4eda
- https://git.kernel.org/stable/c/4d339b219004869e96c4ce56b8891f83a38da4c0
- https://git.kernel.org/stable/c/639deb962986ef2f5e2a6d5a600c66f922471e81
- https://git.kernel.org/stable/c/7425453ea16dbc3bbb0f6cac4d60b537e5e4d151
- https://git.kernel.org/stable/c/96e53bb3ee2f354cf6b4ab07bcc56e500f8b3f74
- https://git.kernel.org/stable/c/e66dcf7bb9c4df5582c82bc3582725abcbfbea73

- https://git.kernel.org/stable/c/ebbbc4bfad4cb355d17c671223d0814ee3ef4eda
- https://github.com/torvalds/linux/commit/639deb962986ef2f5e2a6d5a600c66f922471e81
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-45972
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11793

60

Краткое описание: Повышение привилегий в Ubuntu

Идентификатор уязвимости: CVE-2026-15226
BDU:2026-11872

Идентификатор программной ошибки: CWE-250 Выполнение операций с избыточными привилегиями

Уязвимый продукт: Ubuntu: 26.04 LTS

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

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://docs.devguard.org/vulnerability-database/CVE-2026-15226/
- https://ubuntu.com/security/CVE-2026-15226
- https://bdu.fstec.ru/vul/2026-11872

61

Краткое описание: Отказ в обслуживании в ImageMagick

Идентификатор уязвимости: CVE-2026-56368
BDU:2026-10481

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

Уязвимый продукт: ImageMagick: до 6.9.13-40
Debian GNU/Linux: 13
РЕД ОС: 8.0

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: 2026-07-21 / 2026-07-21

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-wfx3-6g53-9fgc
- https://security-tracker.debian.org/tracker/CVE-2026-56368
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-10481

62

Краткое описание: Отказ в обслуживании в ImageMagick

Идентификатор уязвимости: CVE-2026-53461
BDU:2026-10449

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: ImageMagick: до 6.9.13-50
Debian GNU/Linux: 13
РЕД ОС: 8.0
АЛЬТ СП 10: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-21 / 2026-07-21

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-g22q-f7gc-5jhr
- https://security-tracker.debian.org/tracker/CVE-2026-53461
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-10449

63

Краткое описание: Получение конфиденциальной информации в Apache Camel

Идентификатор уязвимости: CVE-2026-55994
BDU:2026-10445

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

Уязвимый продукт: Camel: от 4.17.0 до 4.18.3

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

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-55994.html
- https://github.com/oscerd/CVE-2026-55994
- https://bdu.fstec.ru/vul/2026-10445

64

Краткое описание: Получение конфиденциальной информации в Apache Camel

Идентификатор уязвимости: CVE-2026-55993
BDU:2026-10444

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

Уязвимый продукт: Camel: от 4.19.0 до 4.21.0

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

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-55993.html
- https://github.com/oscerd/CVE-2026-55993
- https://bdu.fstec.ru/vul/2026-10444

65

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64600
BDU:2026-10442

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

Уязвимый продукт: Linux: до 7.2-rc4
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8
Red Hat Enterprise Linux for NVIDIA: 26

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/0xBlackash/CVE-2026-64600
- https://1275.ru/vulnerability/uyazvimost-v-xfs-faylovoy-sisteme-yadra-linux-sostoyanie-gonki-pozvolyaet-lokalnomu-polzovatelyu-poluchit-root-prava_32643
- https://git.kernel.org/stable/c/206c09b04dc5469c7ff14d8aceff2d47c88078d9
- https://git.kernel.org/stable/c/2f4acd0fcd862e22eab45690ec2c08c80b6ef2e7
- https://git.kernel.org/stable/c/44f891bc088958399eec27f7604928694aa35581

- https://git.kernel.org/stable/c/e705d81a7193dd19e69b8e2bad4696d78a4ea075
- https://security-tracker.debian.org/tracker/CVE-2026-64600
- https://access.redhat.com/security/cve/cve-2026-64600
- https://www.cve.org/CVERecord?id=CVE-2026-64600
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://bdu.fstec.ru/vul/2026-10442

66

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-55044
BDU:2026-10542

Идентификатор программной ошибки: CWE-125 Чтение за пределами 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: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55044
- https://bdu.fstec.ru/vul/2026-10542

67

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

Идентификатор уязвимости: CVE-2026-50411
BDU:2026-10533

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 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 24H2: до 10.0.26100.8875
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
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: 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50411
- https://bdu.fstec.ru/vul/2026-10533

68

Краткое описание: Выполнение произвольного кода в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-50685
BDU:2026-10537

Идентификатор программной ошибки: CWE-415 Двойное освобождение

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 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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50685
- https://bdu.fstec.ru/vul/2026-10537

69

Краткое описание: Выполнение произвольного кода в Windows OLE

Идентификатор уязвимости: CVE-2026-50686
BDU:2026-10538

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.1 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50686
- https://bdu.fstec.ru/vul/2026-10538

70

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-50688
BDU:2026-10540

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 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50688
- https://bdu.fstec.ru/vul/2026-10540

71

Краткое описание: Повышение привилегий в Windows Clipboard Server

Идентификатор уязвимости: CVE-2026-50689
BDU:2026-10541

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: 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 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: 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-2026-50689

- https://bdu.fstec.ru/vul/2026-10541

72

Краткое описание: Выполнение произвольного кода в Remote Desktop Protocol

Идентификатор уязвимости: CVE-2026-56190
BDU:2026-10545

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56190
- https://bdu.fstec.ru/vul/2026-10545

Краткое описание: Получение конфиденциальной информации в ZooKeeper

Идентификатор уязвимости: CVE-2026-24308
BDU:2026-10568

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

Уязвимый продукт: РЕД ОС: 8.0
ZooKeeper: от 3.8.0 до 3.8.5 включительно
Platform V IAM SE: до 2.3.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Ссылки на источник:

- https://www.openwall.com/lists/oss-security/2026/03/07/5
- https://lists.apache.org/thread/qng3rtzv2pqkmko4rhv85jfplkyrgqdr
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-24308
- https://bdu.fstec.ru/vul/2026-10568

74

Краткое описание: Повышение привилегий в Gitea

Идентификатор уязвимости: CVE-2026-20706
BDU:2026-10565

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

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: 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: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://blog.Gitea.com/release-of-1.26.2/
- https://github.com/advisories/GHSA-cr4g-f395-h25h
- https://github.com/go-Gitea/Gitea
- https://github.com/go-Gitea/Gitea/pull/37735
- https://github.com/go-Gitea/Gitea/releases/tag/v1.26.2
- https://github.com/go-Gitea/Gitea/security/advisories/GHSA-cr4g-f395-h25h
- https://nvd.nist.gov/vuln/detail/CVE-2026-20706
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-20706
- https://bdu.fstec.ru/vul/2026-10565

Краткое описание: Выполнение произвольного кода в Windows Active Directory Federation Services

Идентификатор уязвимости: CVE-2026-55055
BDU:2026-10572

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: Операционные системы Microsoft и их компоненты

75

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50355
- https://bdu.fstec.ru/vul/2026-10572

76

Краткое описание: Отказ в обслуживании в Netty

Идентификатор уязвимости: CVE-2026-56819
BDU:2026-10489

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

Уязвимый продукт: Netty: от 4.1.0.Final до 4.1.135.Final включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/netty/netty/security/advisories/GHSA-93wv-jw9v-4972
- https://github.com/netty/netty/releases/tag/netty-4.1.136.Final
- https://github.com/netty/netty/releases/tag/netty-4.2.16.Final
- https://bdu.fstec.ru/vul/2026-10489

77

Краткое описание: Выполнение произвольного кода в Redis

Идентификатор уязвимости: CVE-2026-66373
BDU:2026-10490

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Redis: до 8.8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/redis/redis/compare/8.6.4...8.8.0
- https://github.com/redis/redis/pull/15081
- https://github.com/berabuddies/redis-poc
- https://bdu.fstec.ru/vul/2026-10490

78

Краткое описание: Выполнение произвольного кода в FastJson

Идентификатор уязвимости: CVE-2026-16723
BDU:2026-10492

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: FastJson: от 1.2.68 до 1.2.83

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: 9.0 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: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://github.com/alibaba/fastjson2/wiki/Security-Advisory:-Remote-Code-Execution-in-fastjson-1.2.68%E2%80%931.2.83
- https://thehackernews.com/2026/07/fastjson-1x-rce-vulnerability-targeted.html
- https://github.com/HORKimhab/CVE-2026-16723
- https://bdu.fstec.ru/vul/2026-10492

79

Краткое описание: Выполнение произвольного кода в Check Point SmartConsole

Идентификатор уязвимости: CVE-2026-16232
BDU:2026-10493

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Security Management Server: до R82
Check Point SmartConsole: -
Multi-Domain Security Management Server (MDS): до R82.10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://support.checkpoint.com/results/sk/sk185169/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-16232
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-10493

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2023-53751
BDU:2026-10612

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.0 до 6.1.27 включительно
Red Hat Enterprise Linux: 8.4 Extended Update Support Long-Life Add-On
Debian GNU/Linux: 12

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.

80

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: 2026-07-21 / 2026-07-21

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2023-53751
- https://git.kernel.org/stable/c/64d62ac6d6514cba1305bd08e271ec1843bdd612
- https://git.kernel.org/stable/c/c511954bf142fe1995aec3c739a9f1a76990283a
- https://git.kernel.org/stable/c/0b08c4c499200be67d54c439d56e5ea866869945
- https://git.kernel.org/linus/90c49fce1c43e1cc152695e20363ff5087897c09
- https://lore.kernel.org/linux-cve-announce/2025120842-CVE-2023-53751-2ff2@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2023-53751
- https://access.redhat.com/security/cve/cve-2023-53751
- https://bdu.fstec.ru/vul/2026-10612

81

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23234
BDU:2026-10616

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.19 до 6.19.2 включительно
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8
Альт 8 СП: -
АЛЬТ СП 10: -

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-21 / 2026-07-21

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23234
- https://git.kernel.org/stable/c/0fb58aff0dafd6837cc91f4154f3ed6e020358fa
- https://git.kernel.org/stable/c/2f67ff1e15a8a4d0e4ffc6564ab20d03d7398fe9
- https://git.kernel.org/stable/c/505e1c0530db6152cab3feef8e3e4da3d3e358c9
- https://git.kernel.org/stable/c/acc2c97fc0005846e5cf11b5ba3189fef130c9b3
- https://git.kernel.org/stable/c/cf4a9e1bc8129eb63fda5f8bdcd8d87f0bd76f42
- https://git.kernel.org/stable/c/995030be4ce6338c6ff814583c14166446a64008

- https://git.kernel.org/stable/c/a42f99be8a16b32a0bb91bb6dda212a6ad61be5d
- https://git.kernel.org/linus/ce2739e482bce8d2c014d76c4531c877f382aa54
- https://lore.kernel.org/linux-cve-announce/2026030439-CVE-2026-23234-5cef@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-23234
- https://altsp.su/obnovleniya-bezopasnosti/
- https://altsp.su/obnovleniya-bezopasnosti/
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-10616

82

Краткое описание: Отказ в обслуживании в Lexbor

Идентификатор уязвимости: CVE-2026-29079
BDU:2026-02724

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

Уязвимый продукт: Lexbor: 2.6.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://github.com/lexbor/lexbor/commit/fbb91d229722064e254e8ef3d70289868520da25
- https://github.com/php/php-src/blob/80f06614ffccabdf18fac591e2bdec03362f7ff8/NEWS#L52-L53
- https://github.com/lexbor/lexbor/security/advisories/GHSA-mrpr-v36q-2vp8
- https://bdu.fstec.ru/vul/2026-02724

83

Краткое описание: Чтение локальных файлов в Apache Camel

Идентификатор уязвимости: CVE-2026-48204
BDU:2026-10608

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Camel: от 4.19.0 до 4.21.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv3: 9.8 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://camel.apache.org/security/CVE-2026-48204.html
- https://github.com/oscerd/CVE-2026-48204
- https://bdu.fstec.ru/vul/2026-10608

84

Краткое описание: Повышение привилегий в Windows Narrator Braille

Идентификатор уязвимости: CVE-2026-58635
BDU:2026-10604

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

Уязвимый продукт: 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 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: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58635
- https://github.com/DavidCarliez/CVE-2026-58635-PoC
- https://bdu.fstec.ru/vul/2026-10604

85

Краткое описание: Повышение привилегий в Windows User Interface Core

Идентификатор уязвимости: CVE-2026-50454
BDU:2026-10603

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/DavidCarliez/Windows-AppResolver-LPE-PoC
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50454
- https://bdu.fstec.ru/vul/2026-10603

86

Краткое описание: Выполнение произвольного кода в Microsoft Message Queuing Queue Manager

Идентификатор уязвимости: CVE-2026-54992
BDU:2026-10602

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.4 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54992
- https://github.com/DavidCarliez/CVE-2026-54992-PoC
- https://bdu.fstec.ru/vul/2026-10602

87

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2023-54207
BDU:2026-10609

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 5.11 до 5.15.198 включительно
Red Hat Enterprise Linux: 9
Debian GNU/Linux: 12
Альт 8 СП: -

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: 2026-07-21 / 2026-07-21

Ссылки на источник:

- https://git.kernel.org/stable/c/4c2707dfee5847dc0b5ecfbe512c29c93832fdc4
- https://git.kernel.org/stable/c/f283805d984343b2f216e2f4c6c7af265b9542ae
- https://git.kernel.org/stable/c/51f49e3927ad545cec0c0afb86856ccacd9f085d
- https://git.kernel.org/stable/c/f78bb490b16ecb506d4904be4b00bf9aad6588f9
- https://git.kernel.org/stable/c/58f0d1c0e494a88f301bf455da7df4366f179bbb
- https://www.cve.org/CVERecord?id=CVE-2023-54207
- https://git.kernel.org/linus/dd613a4e45f8d35f49a63a2064e5308fa5619e29
- https://lore.kernel.org/linux-cve-announce/2025123023-CVE-2023-54207-8b3a@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2023-54207
- https://access.redhat.com/security/cve/cve-2023-54207
- https://altsp.su/obnovleniya-bezopasnosti/
- https://bdu.fstec.ru/vul/2026-10609

88

Краткое описание: Выполнение произвольного кода в Rclone

Идентификатор уязвимости: CVE-2026-41179
BDU:2026-10664

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

Уязвимый продукт: Rclone: от 1.48.0 до 1.73.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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/rclone/rclone/security/advisories/GHSA-jfwf-28xr-xw6q
- https://github.com/rclone/rclone/releases/tag/v1.73.5
- https://github.com/rclone/rclone/commit/2a9e952b38e03a96bf40c9eb6e8e22199865ee3b
- https://github.com/rclone/rclone/blob/bf55d5e6d37fd86164a87782191f9e1ffcaafa82/fs/rc/cache.go
- https://github.com/rclone/rclone/blob/bf55d5e6d37fd86164a87782191f9e1ffcaafa82/fs/operations/rc.go
- https://github.com/rclone/rclone/blob/bf55d5e6d37fd86164a87782191f9e1ffcaafa82/backend/webdav/webdav.go
- https://365trust.me/rclone-proof-of-concepts-pocs-are-available-for-exploiting-cve-2026-41176-and-cve-2026-41179-al02-260427-csirt-ita/
- https://bdu.fstec.ru/vul/2026-10664

89

Краткое описание: Выполнение произвольного кода в Metabase

Идентификатор уязвимости: CVE-2026-59827
BDU:2026-10663

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Metabase: от 1.61.0 до 1.61.1.4

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/metabase/metabase/commit/00f42511fe3bc4385652a2e96862ee6fd7d42cf8
- https://github.com/metabase/metabase/releases/tag/v0.58.15
- https://github.com/metabase/metabase/releases/tag/v0.59.12
- https://github.com/metabase/metabase/releases/tag/v0.60.6.3
- https://github.com/metabase/metabase/releases/tag/v0.61.1.4
- https://github.com/metabase/metabase/security/advisories/GHSA-w95f-x9v9-wv36
- https://securityonline.info/metabase-h2-rce-cve-2026-59827/
- https://cve.circl.lu/sightings/?query=CVE-2026-59827
- https://github.com/pickl31/CVE-2026-59827
- https://github.com/c0gnit00/CVE-2026-59827
- https://bdu.fstec.ru/vul/2026-10663

90

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51302
BDU:2026-10657

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: 3.41

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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51302
- https://github.com/sqlite/sqlite/blob/master/src/expr.c
- https://bdu.fstec.ru/vul/2026-10657

91

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51303
BDU:2026-10661

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: до 3.51.3

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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51303
- https://github.com/sqlite/sqlite/blob/master/src/expr.c
- https://github.com/sqlite/sqlite/releases/tag/version-3.51.3
- https://bdu.fstec.ru/vul/2026-10661

92

Краткое описание: Выполнение произвольного кода в Flask-Reuploaded

Идентификатор уязвимости: CVE-2026-27641
BDU:2026-10662

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

Уязвимый продукт: Flask-Reuploaded: до 1.5.0

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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/jugmac00/flask-reuploaded/security/advisories/GHSA-65mp-fq8v-56jr
- https://github.com/jugmac00/flask-reuploaded/commit/d64c6b2f71cb73734fc38baa0e3e156926361288
- https://github.com/jugmac00/flask-reuploaded/pull/180
- https://github.com/Max78000/CVE-2026-27641-Flask-Reuploaded
- https://bdu.fstec.ru/vul/2026-10662

93

Краткое описание: Выполнение произвольного кода в OpenWrt

Идентификатор уязвимости: CVE-2026-53921
BDU:2026-10650

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: OpenWrt: до 25.12.5

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://thehackernews.com/2026/07/critical-openwrt-dhcpv6-flaw-could-let.html
- https://github.com/openwrt/odhcpd/security/advisories/GHSA-7fwx-hhrg-3496
- https://bdu.fstec.ru/vul/2026-10650

94

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51297
BDU:2026-10651

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: 3.41

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51297
- https://github.com/sqlite/sqlite/blob/master/src/json.c
- https://bdu.fstec.ru/vul/2026-10651

95

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51296
BDU:2026-10652

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: 3.41

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: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/programmervuln/cveadvisory-/commit/75a435c839a4bcc6ca2ad21e3b07c978d814acb2
- https://github.com/sqlite/sqlite/blob/master/src/json.c
- https://bdu.fstec.ru/vul/2026-10652

96

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-53366
BDU:2026-10626

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.0 до 6.6.144
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8
АЛЬТ СП 10: -

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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://git.kernel.org/linus/eca856950f7cb1a221e02b99d758409f2c5cec42
- https://git.kernel.org/stable/c/77798d7be6ef71e72fb6fc8a2901bf74ebc9706f
- https://git.kernel.org/stable/c/a9c24eda24bd15f432e37824e6fc440977cb241c
- https://git.kernel.org/stable/c/c04d9ece23deb9e26c19f9ca215e98b3295aa1bb
- https://git.kernel.org/stable/c/ce494707a9c07f27c219ca67f3e138061f53d9b3
- https://git.kernel.org/stable/c/eca856950f7cb1a221e02b99d758409f2c5cec42

- https://nvd.nist.gov/vuln/detail/CVE-2026-53366
- https://security-tracker.debian.org/tracker/CVE-2026-53366
- https://wiki.astralinux.ru/x/0IVcHg
- https://wiki.astralinux.ru/x/nIJcHg
- https://wiki.astralinux.ru/x/wYVcHg
- https://wiki.astralinux.ru/x/xYVcHg
- https://wiki.astralinux.ru/x/zIVcHg
- https://security-tracker.debian.org/tracker/CVE-2026-53366
- https://ubuntu.com/security/CVE-2026-53366
- https://access.redhat.com/security/cve/cve-2026-53366
- https://altsp.su/obnovleniya-bezopasnosti/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://bdu.fstec.ru/vul/2026-10626

97

Краткое описание: Выполнение произвольного кода в VMware SD-WAN Orchestrator

Идентификатор уязвимости: CVE-2026-16812
BDU:2026-10655

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

Уязвимый продукт: VMware SD-WAN Orchestrator: от 7.0.0 до 7.0.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Ссылки на источник:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://securityonline.info/velocloud-command-injection-cve-2026-16812/
- https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
- https://www.cve.org/CVERecord?id=CVE-2026-16812
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-10655

98

Краткое описание: Отказ в обслуживании в SQLite

Идентификатор уязвимости: CVE-2026-51300
BDU:2026-10660

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://github.com/programmervuln/cveadvisory-/blob/main/CVE-2026-51300
- https://github.com/sqlite/sqlite/blob/master/src/expr.c
- https://bdu.fstec.ru/vul/2026-10660

99

Краткое описание: Выполнение произвольного кода в SQLite

Идентификатор уязвимости: CVE-2026-51304
BDU:2026-10653

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SQLite: 3.41

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: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/programmervuln/cveadvisory-/blob/main/CVE-2026-51304
- https://github.com/sqlite/sqlite/blob/master/src/expr.c
- https://bdu.fstec.ru/vul/2026-10653

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31669
BDU:2026-10731

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

Уязвимый продукт: Linux: от 5.12 до 5.15.202 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

100

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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://git.kernel.org/stable/c/fb1f54b7d16f393b8b65d328410f78b4beea8fcc
- https://git.kernel.org/stable/c/f6e1f25fa5e733570f6d6fe37a4dfed2a0deba47
- https://git.kernel.org/stable/c/3fd6547f5b8ac99687be6d937a0321efda760597
- https://git.kernel.org/stable/c/b313e9037d98c13938740e5ebda7852929366dff
- https://git.kernel.org/stable/c/eb9c6aeb512f877cf397deb1e4526f646c70e4a7
- https://git.kernel.org/stable/c/15fa9ead4d5e6b6b9c794e84144146c917f2cb62
- https://www.cve.org/CVERecord?id=CVE-2026-31669
- https://git.kernel.org/linus/9b55b253907e7431210483519c5ad711a37dafa1
- https://lore.kernel.org/linux-cve-announce/2026042406-CVE-2026-31669-0e0d@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-31669
- https://access.redhat.com/security/cve/cve-2026-31669
- https://bdu.fstec.ru/vul/2026-10731

101

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31668
BDU:2026-10732

Идентификатор программной ошибки: CWE-821 Некорректная синхронизация

Уязвимый продукт: Linux: от 4.10 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 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: 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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://git.kernel.org/stable/c/57d0374d14fa667dec6952173b93e7e84486d5c9
- https://git.kernel.org/stable/c/17d87d42874f5d6c1a0ccc6d9190dfe82a9a7a6a
- https://git.kernel.org/stable/c/84d458018b147176b259347103fccb7e93abd2b1
- https://git.kernel.org/stable/c/750569d6987a0ff46317a4b86eb3907e296287bf
- https://git.kernel.org/stable/c/6305ad032b03d2ea4181b953a66e19a9a6ed053c
- https://git.kernel.org/stable/c/1dec91d3b1cefb82635761b7812154af3ef46449
- https://git.kernel.org/stable/c/fb56de5d99218de49d5d43ef3a99e062ecd0f9a1
- https://www.cve.org/CVERecord?id=CVE-2026-31668
- https://git.kernel.org/linus/c3812651b522fe8437ebb7063b75ddb95b571643

- https://lore.kernel.org/linux-cve-announce/2026042406-CVE-2026-31668-50e7@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31668
- https://access.redhat.com/security/cve/cve-2026-31668
- https://bdu.fstec.ru/vul/2026-10732

102

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31657
BDU:2026-10733

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 3.5 до 6.1.168 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 9.8 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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://git.kernel.org/stable/c/7962b522222628596ca9ecc8722efc95367aadbd
- https://git.kernel.org/stable/c/2f55b58b5a0bbed192d60c444a45a49cdf1b545f
- https://git.kernel.org/stable/c/f4858832ddef2f39f21e30b7226bbcd3c4b2bc96
- https://git.kernel.org/stable/c/4dee4c0688443aaf5bbec74aa203c851d1d53c35
- https://git.kernel.org/stable/c/1f2dc36c297d27733f1b380ea644cf15a361bd7b
- https://www.cve.org/CVERecord?id=CVE-2026-31657
- https://git.kernel.org/linus/82d8701b2c930d0e96b0dbc9115a218d791cb0d2
- https://lore.kernel.org/linux-cve-announce/2026042402-CVE-2026-31657-fbab@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31657
- https://bdu.fstec.ru/vul/2026-10733

103

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23191
BDU:2026-10734

Идентификатор программной ошибки: CWE-667 Некорректная блокировка

Уязвимый продукт: Linux: от 6.13 до 6.18.9 включительно
Red Hat Enterprise Linux: 9.6 Extended Update Support
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.8 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/5727ccf9d19ca414cb76d9b647883822e2789c2e
- https://git.kernel.org/stable/c/bad15420050db1803767e58756114800cce91ea4
- https://www.cve.org/CVERecord?id=CVE-2026-23191
- https://git.kernel.org/linus/826af7fa62e347464b1b4e0ba2fe19a92438084f
- https://lore.kernel.org/linux-cve-announce/2026021433-CVE-2026-23191-f990@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-23191
- https://access.redhat.com/security/cve/cve-2026-23191
- https://bdu.fstec.ru/vul/2026-10734

104

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31785
BDU:2026-10735

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Linux: от 6.19 до 6.19.11 включительно

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31785
- https://git.kernel.org/stable/c/b656f040ed4ed2074dfb78072745b41d44368be0
- https://git.kernel.org/stable/c/6d192b4f2d644d15d9a9f1d33dab05af936f6540
- https://lore.kernel.org/linux-cve-announce/2026050152-CVE-2026-31785-e014@gregkh/
- https://bdu.fstec.ru/vul/2026-10735

105

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31748
BDU:2026-10736

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 2.6.29 до 5.10.252 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 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.cve.org/CVERecord?id=CVE-2026-31748
- https://git.kernel.org/stable/c/2fc25a4c2e055cd42ea39a1b42c89bfef70e0319
- https://git.kernel.org/stable/c/9f39fa07259eb342908e4aa0271dee038a8ce4f8
- https://git.kernel.org/stable/c/f3f8ec00cfb8d8e826e30b1138a56355b88e9ba8
- https://git.kernel.org/stable/c/c16ac4e173a05011437a2d868f70cc415339065a
- https://git.kernel.org/stable/c/1bf8761eb59e94bf7b8c17b2a1ee48f14378b172
- https://git.kernel.org/stable/c/a47ae40339c1048f519df33ff8840731720f57cb
- https://git.kernel.org/stable/c/c8c607a77aab783f2e38cc2e0f24aa6c8f6d200b
- https://git.kernel.org/stable/c/cc797d4821c754c701d9714b58bea947e31dbbe0
- https://lore.kernel.org/linux-cve-announce/2026050141-CVE-2026-31748-ab3e@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-31748
- https://bdu.fstec.ru/vul/2026-10736

106

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31735
BDU:2026-10738

Идентификатор программной ошибки: CWE-459 Неполная очистка

Уязвимый продукт: Linux: от 6.19 до 6.19.11 включительно

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31735
- https://git.kernel.org/stable/c/50ecd96a28f712f8b682c0441f4cb9b086d28816
- https://git.kernel.org/stable/c/ee6e69d032550687a3422504bfca3f834c7b5061
- https://lore.kernel.org/linux-cve-announce/2026050138-CVE-2026-31735-436c@gregkh/
- https://bdu.fstec.ru/vul/2026-10738

107

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-55141
BDU:2026-10740

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Office Online Server: до 16.0.10417.20175
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.111.26071215
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: 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-2026-55141
- https://bdu.fstec.ru/vul/2026-10740

108

Краткое описание: Выполнение произвольного кода в DHCP Server Service

Идентификатор уязвимости: CVE-2026-56159
BDU:2026-10741

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56159
- https://bdu.fstec.ru/vul/2026-10741

109

Краткое описание: Выполнение произвольного кода в Windows Resilient File System

Идентификатор уязвимости: CVE-2026-58530
BDU:2026-10745

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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-2026-58530
- https://bdu.fstec.ru/vul/2026-10745

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31705
BDU:2026-10730

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19 до 7.0.1 включительно
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://git.kernel.org/stable/c/30010c952077a1c89ecdd71fc4d574c75a8f5617
- https://git.kernel.org/stable/c/98f3de6ef4efbd899348d333f0902dc4ff14380c
- https://git.kernel.org/stable/c/922d48fe8c19f388ffa2f709f33acaae4e408de2
- https://git.kernel.org/stable/c/ffbce350c6fd1e99116ea57383b9031717e36d3b
- https://git.kernel.org/stable/c/790304c02bf9bd7b8171feda4294d6e62d32ae8f
- https://www.cve.org/CVERecord?id=CVE-2026-31705
- https://lore.kernel.org/linux-cve-announce/2026050121-CVE-2026-31705-5bdc@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31705
- https://bdu.fstec.ru/vul/2026-10730

111

Краткое описание: Повышение привилегий в Windows Sensor Data Service

Идентификатор уязвимости: CVE-2026-50367
BDU:2026-10747

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: 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 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: 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50367

- https://bdu.fstec.ru/vul/2026-10747

112

Краткое описание: Обход безопасности в Windows Secure Boot

Идентификатор уязвимости: CVE-2026-49783
BDU:2026-10748

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

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: Злоупотребление функционалом.

Последствия эксплуатации: Обход безопасности

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

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49783
- https://bdu.fstec.ru/vul/2026-10748

113

Краткое описание: Выполнение произвольного кода в Microsoft Windows Media Foundation

Идентификатор уязвимости: CVE-2026-50655
BDU:2026-10751

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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-2026-50655
- https://bdu.fstec.ru/vul/2026-10751

114

Краткое описание: Повышение привилегий в Windows Network Connections Service

Идентификатор уязвимости: CVE-2026-50476
BDU:2026-10753

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 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26200.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50476
- https://bdu.fstec.ru/vul/2026-10753

115

Краткое описание: Повышение привилегий в Windows Overlay Filter

Идентификатор уязвимости: CVE-2026-50435
BDU:2026-10755

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: 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-2026-50435
- https://bdu.fstec.ru/vul/2026-10755

116

Краткое описание: Повышение привилегий в Windows Win32 Kernel Subsystem

Идентификатор уязвимости: CVE-2026-58632
BDU:2026-10758

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: 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58632
- https://bdu.fstec.ru/vul/2026-10758

117

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-56176
BDU:2026-10742

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56176
- https://bdu.fstec.ru/vul/2026-10742

118

Краткое описание: Повышение привилегий в Windows DHCP Client

Идентификатор уязвимости: CVE-2026-49181
BDU:2026-10746

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 7.5 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49181
- https://bdu.fstec.ru/vul/2026-10746

119

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31747
BDU:2026-10737

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

Уязвимый продукт: Linux: от 3.19 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: 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.cve.org/CVERecord?id=CVE-2026-31747
- https://git.kernel.org/stable/c/8ddfe6495c245226a30d8b36e2f4a7aa7712e8d6
- https://git.kernel.org/stable/c/64b24b713e1a3ea6624480594b4f8c2ff86502f2
- https://git.kernel.org/stable/c/f72b5567f7c117b46b4058dc6a0c7554f8565561
- https://git.kernel.org/stable/c/1603dd471f47762e9d1f52304edb3e49a7e62655
- https://git.kernel.org/stable/c/99f31aa98ab6e3805c455b65bcd01b3d48bdf1a5
- https://git.kernel.org/stable/c/eae19cab44204537f79146f15a51811b13227c38
- https://git.kernel.org/stable/c/de3f923ae7d91480ed3ecea1b1e1fc0dc25b597d
- https://git.kernel.org/stable/c/3fb43a7a5b44713f892c58ead2e5f3a1bc9f4ee7
- https://lore.kernel.org/linux-cve-announce/2026050141-CVE-2026-31747-430e@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-31747
- https://bdu.fstec.ru/vul/2026-10737

120

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43379
BDU:2026-10721

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 6.19.8 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: 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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43379
- https://git.kernel.org/stable/c/bf4d66d72e4a9e268c1012c331ce9eaedb5e2086
- https://git.kernel.org/stable/c/960699317d39f46611f4ebeb69edc567c1f4e6b6
- https://git.kernel.org/stable/c/dbbd328cf58261ca239756fe1c0d10c9518d3399
- https://git.kernel.org/stable/c/b3568347c51c46e2cabc356bc34676df98296619
- https://git.kernel.org/linus/eac3361e3d5dd8067b3258c69615888eb45e9f25
- https://lore.kernel.org/linux-cve-announce/2026050832-CVE-2026-43379-1808@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-43379
- https://bdu.fstec.ru/vul/2026-10721

121

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43011
BDU:2026-10728

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

Уязвимый продукт: Linux: от 6.19 до 6.19.11 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43011
- https://git.kernel.org/stable/c/5d0aa038a90b30c9bedde0c41c1fdcd98ecb16e9
- https://git.kernel.org/stable/c/3f5e3005984645bf5bd129c6b13149879580b1fb
- https://git.kernel.org/stable/c/f782dd382203b2a8c4552a628431b7de65a19a7b
- https://git.kernel.org/stable/c/143d4fa68ae9efb83b0c55b12cc7f0d03732a2b1
- https://git.kernel.org/stable/c/524371398d8463ea7e101fce2cbf3915645d1730
- https://git.kernel.org/stable/c/fa1dbc93530b34fab0da9862426fe9c918c74dc0
- https://git.kernel.org/stable/c/c87dd137c0dad07cc55f98181ff380b0c23d2878
- https://git.kernel.org/stable/c/d10a26aa4d072320530e6968ef945c8c575edf61
- https://lore.kernel.org/linux-cve-announce/2026050155-CVE-2026-43011-dc56@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-43011
- https://bdu.fstec.ru/vul/2026-10728

122

Краткое описание: Выполнение произвольного кода в PT Application Inspector (PT AI)

Идентификатор уязвимости: BDU:2026-10684

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

Уязвимый продукт: PT Application Inspector (PT AI): -
AI.Plugin.Azure: до 1.3.1 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L

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://github.com/POSIdev-community/AI.Plugin.Azure/releases/tag/v1.3.2
- https://bdu.fstec.ru/vul/2026-10684

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31718
BDU:2026-10729

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.9 до 6.12.83 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.

123

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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-31718
- https://git.kernel.org/stable/c/e33c65f011980b4ad4abfd93585ec2079856368f
- https://git.kernel.org/stable/c/3d6682726c2d3a46d31dae88b8166786b09b03ad
- https://git.kernel.org/stable/c/b34fc42cfe922e551f7a27d3ac3bb016e41d7dd9
- https://git.kernel.org/stable/c/235e32320a470fcd3998fb3774f2290a0eb302a1
- https://lore.kernel.org/linux-cve-announce/2026050124-CVE-2026-31718-5752@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-31718
- https://bdu.fstec.ru/vul/2026-10729

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23450
BDU:2026-10720

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 6.19 до 6.19.9 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.

124 **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: 2026-07-22 / 2026-07-22

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23450
- https://git.kernel.org/stable/c/1e4f873879e075bbd4eb1c644d6933303ac5eba4
- https://git.kernel.org/stable/c/f00fc26c8a06442b225a350fe000c0a11483e6a3
- https://git.kernel.org/stable/c/cadf3da46c15523fba90d80c9955f536ee3b4023
- https://git.kernel.org/stable/c/fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2
- https://git.kernel.org/stable/c/1fab5ece76fb42a761178dcd0ebcbf578377b0dd
- https://git.kernel.org/linus/6d5e4538364b9ceb1ac2941a4deb86650afb3538
- https://lore.kernel.org/linux-cve-announce/2026040316-CVE-2026-23450-2437@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2026-23450

- https://access.redhat.com/security/cve/cve-2026-23450
- https://bdu.fstec.ru/vul/2026-10720

125

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-54107
BDU:2026-10699

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование 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: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54107
- https://github.com/Pravin761/CVE-2026-54107
- https://bdu.fstec.ru/vul/2026-10699

126

Краткое описание: Повышение привилегий в Airflow Fab Provider

Идентификатор уязвимости: CVE-2026-59243
BDU:2026-10701

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Airflow Fab Provider: до 3.7.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.8 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://lists.apache.org/thread/x4784l7z00tl3gw4tv2dmvoon77rxgpl
- https://github.com/MalHyuk/CVE-2026-59243
- http://openwall.com/lists/oss-security/2026/07/28/10
- https://github.com/apache/airflow/pull/69374
- https://bdu.fstec.ru/vul/2026-10701

127

Краткое описание: Отказ в обслуживании в cJSON

Идентификатор уязвимости: CVE-2026-67215
BDU:2026-10702

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: cJSON: до 1.7.19

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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://github.com/DaveGamble/cJSON/blob/v1.7.19/cJSON_Utils.c#L906-L940
- https://github.com/DaveGamble/cJSON/blob/v1.7.19/cJSON.c#L253-L261
- https://www.vulncheck.com/advisories/cjson-json-patch-copy-add-uncontrolled-recursion-stack-exhaustion
- https://joshua.hu/cjson-json-parser-cve-vulnerabilities
- https://bdu.fstec.ru/vul/2026-10702

Краткое описание: Выполнение произвольного кода в Gitea

Идентификатор уязвимости: CVE-2026-60004
BDU:2026-10703

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

Уязвимый продукт: Gitea: от 1.17 до 1.27.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

128

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://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m
- https://github.com/HORKimhab/CVE-2026-60004
- https://thehackernews.com/2026/07/new-gitea-rce-lets-repository-writers.html
- https://bdu.fstec.ru/vul/2026-10703

129

Краткое описание: Выполнение произвольного кода в MediaWiki

Идентификатор уязвимости: CVE-2026-58025
BDU:2026-10705

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: MediaWiki: до 1.46.0
Debian GNU/Linux: 13

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/shinthink/CVE-2026-58025
- https://github.com/wikimedia/mediawiki/commit/60f154d4618063ac4d5832285fc246b8fcd7c72c
- https://github.com/wikimedia/mediawiki/commit/50755a861e6e748cf8bac24e8cdd5e83db018081
- https://lists.wikimedia.org/hyperkitty/list/mediawiki-announce@lists.wikimedia.org/thread/J52N2ONQO7GP3XR7UIEA5PI7SVZYTBJ7/
- https://security-tracker.debian.org/tracker/CVE-2026-58025
- https://bdu.fstec.ru/vul/2026-10705

130

Краткое описание: Выполнение произвольного кода в Ruby on Rails

Идентификатор уязвимости: CVE-2026-66066
BDU:2026-10713

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

Уязвимый продукт: Ruby on Rails: от 8.1.0 до 8.1.3.1
libvips: до 8.13
Active Storage: от 7.0.0 до 7.2.3.2
ruby-vips: до 2.2.1

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: 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: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://ethiack.com/info-hub/research/kindarails2shell-rails-rce-cve-2026-66066
- https://discuss.rubyonrails.org/t/cve-2026-66066-possible-arbitrary-file-read-and-remote-code-execution-in-active-storage-variant-processing/91432
- https://thehackernews.com/2026/07/critical-rails-flaw-could-let.html
- https://github.com/rails/rails/security/advisories/GHSA-xr9x-r78c-5hrm
- https://www.libvips.org/2022/05/28/What's-new-in-8.13.html#blocking-of-unfuzzed-loaders
- https://blog.flatt.tech/entry/kindarails2shell_rails
- https://bdu.fstec.ru/vul/2026-10713