НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-08-27.1 | 27 августа 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-31622	Linux	Смежная сеть	ACE	2026-08-10	✓
2	Высокая	CVE-2026-43110	Linux	Смежная сеть	ACE	2026-08-07	✓
3	Критическая	CVE-2026-31478	Linux	Сетевой	ACE	2026-08-07	✓
4	Высокая	CVE-2026-46116	Linux	Локальный	ACE	2026-08-10	✓
5	Высокая	BDU:2026-11285	Linux	Локальный	DoS	2026-08-10	✓
6	Критическая	CVE-2026-23240	Linux	Сетевой	ACE	2026-08-04	✓
7	Высокая	CVE-2026-12326	Firefox	Сетевой	DoS	2026-08-10	✓
8	Критическая	CVE-2026-12293	Firefox	Сетевой	DoS	2026-08-10	✓
9	Критическая	CVE-2026-72529	TrueConf Server	Сетевой	PE	Не определено	✓
10	Критическая	CVE-2026-72530	TrueConf Server	Сетевой	ACE	Не определено	✓
11	Высокая	BDU:2026-11249	MaxPatrol SIEM	Смежная сеть	PE	2025-01-27	✓
12	Критическая	CVE-2026-12316	Firefox	Сетевой	CI	2026-08-10	✓

13	Высокая	CVE-2026-12317	Firefox	Сетевой	DoS	2026-08-10	✓
14	Критическая	CVE-2026-14241	Firefox	Сетевой	DoS	2026-08-10	✓
15	Высокая	CVE-2026-31504	Linux	Локальный	DoS	2026-08-10	✓
16	Высокая	CVE-2026-6758	Firefox	Сетевой	DoS	2026-08-10	✓
17	Высокая	CVE-2026-6782	Firefox	Сетевой	OSI	2026-08-10	✓
18	Высокая	CVE-2026-8952	Firefox	Сетевой	DoS	2026-08-10	✓
19	Высокая	CVE-2026-8963	Firefox	Сетевой	CI	2026-08-10	✓
20	Высокая	CVE-2026-8964	Firefox	Сетевой	CI	2026-08-10	✓
21	Высокая	CVE-2026-8965	Firefox	Сетевой	OSI	2026-08-10	✓
22	Высокая	CVE-2026-8966	Firefox	Сетевой	OSI	2026-08-10	✓
23	Высокая	CVE-2026-8967	Firefox	Сетевой	OSI	2026-08-10	✓
24	Высокая	CVE-2026-8969	Firefox	Сетевой	CI	2026-08-10	✓
25	Высокая	CVE-2026-8972	Firefox	Сетевой	DoS	2026-08-10	✓
26	Высокая	CVE-2026-8973	Firefox	Сетевой	DoS	2026-08-10	✓
27	Высокая	CVE-2026-64560	Linux	Локальный	PE	2026-08-10	✓

28	Высокая	CVE-2026-71324	Traefik	Сетевой	OSI	2026-08-10	✓
29	Высокая	BDU:2026-11282	Clam Antivirus	Сетевой	DoS	2026-08-07	✓
30	Высокая	BDU:2026-11284	Clam Antivirus	Сетевой	ACE	2026-08-07	✓
31	Высокая	CVE-2026-59197	Pillow	Сетевой	OAF	2026-07-16	✓
32	Высокая	CVE-2026-8960	Firefox	Сетевой	LoI	2026-08-10	✓
33	Критическая	CVE-2026-6768	Firefox	Сетевой	DoS	2026-08-10	✓
34	Высокая	CVE-2026-57091	Windows File History Service	Локальный	PE	2026-08-06	✓
35	Высокая	CVE-2026-57089	Windows SMB Server Network Transport Driver	Сетевой	ACE	2026-08-06	✓
36	Критическая	CVE-2026-56188	Windows Server Network driver	Сетевой	ACE	2026-08-05	✓
37	Высокая	CVE-2026-55947	Office Online Server	Локальный	ACE	2026-08-05	✓
38	Критическая	CVE-2026-55944	Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central	Сетевой	ACE	2026-08-05	✓
39	Высокая	CVE-2026-50680	Windows Hyper-V	Локальный	PE	2026-08-05	✓
40	Высокая	CVE-2026-50651	.NET	Сетевой	DoS	2026-08-05	✓
41	Высокая	CVE-2026-50457	Windows Runtime	Локальный	PE	2026-08-05	✓
42	Высокая	CVE-2026-50328	Windows Server	Сетевой	ACE	2026-08-05	✓

43	Высокая	CVE-2026-50388	Windows NTFS	Локальный	ACE	2026-08-05	✓
44	Критическая	CVE-2026-16411	Firefox	Сетевой	ACE	2026-08-04	✓
45	Критическая	CVE-2026-16360	Firefox	Сетевой	ACE	2026-08-04	✓
46	Критическая	CVE-2026-64564	Linux	Сетевой	PE	2026-08-10	✓
47	Высокая	CVE-2026-64561	Linux	Локальный	ACE	2026-08-10	✓
48	Критическая	CVE-2026-62896	Microsoft Teams	Сетевой	PE	2026-08-11	✓
49	Критическая	CVE-2026-50481	Azure Active Directory	Сетевой	PE	2026-08-11	✓
50	Критическая	CVE-2026-68823	Azure Confidential Ledger	Сетевой	ACE	2026-08-11	✓
51	Критическая	CVE-2026-56161	Azure Logic Apps	Сетевой	OSI	2026-08-11	✓
52	Критическая	CVE-2026-50515	Azure Service Bus	Сетевой	ACE	2026-08-11	✓
53	Критическая	CVE-2026-56162	Azure SQL Database	Сетевой	PE	2026-08-11	✓
54	Критическая	CVE-2026-62836	Azure SQL Managed Instance	Сетевой	PE	2026-08-11	✓
55	Критическая	CVE-2026-62830	Azure SRE Agent	Сетевой	PE	2026-08-11	✓
56	Высокая	CVE-2026-64912	Microsoft Access	Локальный	ACE	2026-08-12	✓
57	Высокая	CVE-2026-70345	Windows Installer	Локальный	PE	2026-08-12	✓

58	Высокая	CVE-2026-58641	.NET	Локальный	PE	2026-08-12	✓
59	Критическая	CVE-2026-70332	Microsoft Office SharePoint	Сетевой	SB	2026-08-11	✓
60	Высокая	CVE-2026-62918	Microsoft Teams	Сетевой	SB	2026-08-11	✓
61	Критическая	CVE-2026-62873	Microsoft 365 Admin Center	Сетевой	PE	2026-08-11	✓
62	Критическая	CVE-2026-65667	Microsoft Teams	Сетевой	PE	2026-08-11	✓
63	Высокая	CVE-2026-65773	Windows Kernel	Локальный	PE	2026-08-12	✓
64	Высокая	CVE-2026-62894	Windows DWM Core Library	Локальный	PE	2026-08-12	✓
65	Высокая	CVE-2026-48048	XWiki Platform	Сетевой	OSI	2026-08-12	✓
66	Критическая	CVE-2026-17566	pgAdmin 4	Сетевой	CI	2026-08-12	✓
67	Высокая	CVE-2026-64903	Microsoft Office	Локальный	ACE	2026-08-11	✓
68	Высокая	CVE-2026-61349	Windows Work Folder Service	Локальный	PE	2026-08-12	✓
69	Высокая	CVE-2026-62754	Windows Kerberos	Локальный	PE	2026-08-12	✓
70	Высокая	CVE-2026-62783	Windows Remote Access Connection Manager	Локальный	PE	2026-08-12	✓
71	Высокая	CVE-2026-62822	Windows GDI+	Сетевой	ACE	2026-08-12	✓
72	Высокая	CVE-2026-62823	Windows DHCP Server	Смежная сеть	ACE	2026-08-12	✓

73	Высокая	CVE-2026-64638	Debian GNU/Linux	Сетевой	ACE	2026-08-12	✓
74	Высокая	CVE-2026-68803	Microsoft Excel	Локальный	ACE	2026-08-12	✓
75	Высокая	CVE-2026-70329	Microsoft Outlook	Сетевой	ACE	2026-08-12	✓
76	Высокая	CVE-2026-62885	Windows Win32k	Локальный	PE	2026-08-12	✓
77	Высокая	CVE-2026-62735	Windows HTTP.sys	Локальный	PE	2026-08-12	✓
78	Высокая	CVE-2026-70344	Windows Installer	Локальный	PE	2026-08-12	✓
79	Высокая	CVE-2026-62752	Windows Kerberos	Локальный	PE	2026-08-12	✓
80	Высокая	CVE-2026-62747	Windows Device Association Service	Локальный	PE	2026-08-12	✓
81	Высокая	CVE-2026-62784	Microsoft Local Security Authority Server	Сетевой	ACE	2026-08-12	✓
82	Высокая	CVE-2026-65786	Desktop Window Manager	Локальный	PE	2026-08-12	✓
83	Высокая	CVE-2026-20349	Adaptive Security Appliance	Сетевой	DoS	2026-08-13	✓
84	Высокая	CVE-2026-62700	Windows NTFS	Локальный	PE	2026-08-12	✓
85	Высокая	CVE-2026-62701	Windows Telephony Service	Локальный	PE	2026-08-12	✓
86	Высокая	CVE-2026-62800	Windows SMBv3 Server	Сетевой	ACE	2026-08-12	✓
87	Высокая	CVE-2026-62777	Windows License Manager	Локальный	PE	2026-08-12	✓

88	Высокая	CVE-2026-62779	Windows Schannel	Локальный	PE	2026-08-12	✓
89	Критическая	CVE-2026-46924	Application Testing Suite	Сетевой	ACE	2026-07-22	✓
90	Высокая	CVE-2026-60175	Database Server	Сетевой	ACE	2026-07-22	✓
91	Критическая	CVE-2026-46983	Retail Integration Bus	Сетевой	ACE	2026-07-22	✓
92	Критическая	CVE-2026-46875	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-06	✓
93	Критическая	CVE-2026-35290	Oracle Application Testing Suite	Сетевой	ACE	2026-07-22	✓
94	Критическая	CVE-2026-46876	Oracle Application Testing Suite	Сетевой	ACE	2026-07-22	✓
95	Критическая	CVE-2026-46989	Enterprise Manager Base Platform	Сетевой	DoS	2026-07-22	✓
96	Критическая	CVE-2026-47040	Database Server	Сетевой	DoS	2026-07-22	✓
97	Высокая	CVE-2026-47031	E-Business Suite	Сетевой	ACE	2026-07-22	✓
98	Высокая	CVE-2026-47004	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-22	✓
99	Высокая	CVE-2026-46992	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-22	✓
100	Высокая	CVE-2026-46995	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-22	✓
101	Критическая	CVE-2026-46994	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-22	✓
102	Критическая	CVE-2026-46855	Enterprise Manager Base Platform	Сетевой	ACE	2026-07-06	✓

103	Высокая	CVE-2026-65775	Windows Win32k	Локальный	PE	2026-08-12	✓
104	Критическая	CVE-2026-47036	Siebel CRM	Сетевой	ACE	2026-07-22	✓
105	Высокая	CVE-2026-65774	Windows Installer	Локальный	PE	2026-08-12	✓
106	Высокая	CVE-2026-49163	Application Insights Profiler	Сетевой	PE	2026-08-11	✓
107	Высокая	CVE-2026-62758	Windows Remote Access Connection Manager	Локальный	PE	2026-08-12	✓
108	Высокая	CVE-2026-61364	Windows Remote Desktop Services	Локальный	PE	2026-08-12	✓
109	Высокая	CVE-2026-22980	Linux	Локальный	DoS	2026-08-05	✓
110	Высокая	CVE-2026-23025	Linux	Локальный	DoS	2026-08-05	✓
111	Высокая	CVE-2026-23083	Linux	Локальный	DoS	2026-08-05	✓
112	Высокая	CVE-2026-23095	Linux	Сетевой	DoS	2026-08-05	✓
113	Высокая	CVE-2026-23103	Linux	Локальный	DoS	2026-08-05	✓
114	Высокая	CVE-2026-23169	Linux	Локальный	DoS	2026-08-05	✓
115	Высокая	CVE-2026-23172	Linux	Локальный	DoS	2026-08-05	✓
116	Высокая	CVE-2026-23178	Linux	Локальный	DoS	2026-08-05	✓
117	Высокая	CVE-2026-23193	Linux	Сетевой	DoS	2026-08-05	✓

118	Высокая	CVE-2026-23198	Linux	Локальный	DoS	2026-08-05	✓
119	Высокая	CVE-2026-23105	Linux	Локальный	DoS	2026-08-05	✓
120	Высокая	CVE-2026-23221	Linux	Локальный	DoS	2026-08-05	✓
121	Высокая	CVE-2026-62755	Windows DHCP Client	Локальный	PE	2026-08-12	✓
122	Высокая	CVE-2026-23216	Linux	Локальный	DoS	2026-08-05	✓
123	Высокая	CVE-2026-65668	Microsoft Purview eDiscovery	Сетевой	PE	2026-08-11	✓
124	Критическая	CVE-2026-59118	Copilot Cowork	Сетевой	PE	2026-08-11	✓
125	Критическая	CVE-2026-59115	Microsoft Entra Provisioning Service	Сетевой	PE	2026-08-11	✓
126	Критическая	CVE-2026-63508	Microsoft Planetary Computer Pro	Сетевой	PE	2026-08-10	✓
127	Высокая	CVE-2026-62880	Windows NTFS	Локальный	PE	2026-08-13	✓
128	Высокая	CVE-2026-62819	Windows Routing and Remote Access Service	Сетевой	ACE	2026-08-11	✓
129	Высокая	CVE-2026-62877	Windows Win32k	Локальный	PE	2026-08-13	✓
130	Высокая	CVE-2026-23222	Linux	Локальный	DoS	2026-08-05	✓

1

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31622
BDU:2026-11324

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

Уязвимый продукт: Linux: от 7.0 до 7.0.1
Ubuntu: 26.04 LTS
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.

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/9ba6bb09e00b922d902f684f575779e5433fe6e3
- https://git.kernel.org/stable/c/f83b399aa05a0712e3b1569a30d3d90b3533d2ef
- https://git.kernel.org/stable/c/20663102c14566e900e1d2f679e30b7f1694f387
- https://git.kernel.org/stable/c/2819f34e08bdffb6f06a51c67948ec5737fb166a
- https://git.kernel.org/stable/c/1bec5698b55aa2be5c3b983dba657c01d0fd3dbc
- https://git.kernel.org/stable/c/5a59bf70c38ee1eb4be03bab830bbc3a6f0bd1f1
- https://git.kernel.org/stable/c/8d9d9bf3565271ca7ab9c716a94e87296177e7ba

- https://git.kernel.org/stable/c/cc024a3de265ef6c58957f4990eccb9f806208cb
- https://git.kernel.org/stable/c/46ce8be2ced389bccd84bcc04a12cf2f4d0c22d1
- https://security-tracker.debian.org/tracker/CVE-2026-31622
- https://ubuntu.com/security/CVE-2026-31622
- https://bdu.fstec.ru/vul/2026-11324

2

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43110
BDU:2026-11323

Идентификатор программной ошибки: CWE-1019 Проверка входных данных

Уязвимый продукт: Linux: от 3.9 до 6.6.136
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 24.04 LTS
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.

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/stable/c/1ae1e1caa428844e481231f6dbe9b4f475f1d52d
- https://git.kernel.org/stable/c/2ae3ccb78c0a9ef5ee3d80d02ab319ac1d5af734
- https://git.kernel.org/stable/c/304950a467d83678bd0b0f46331882e2ac23b12d
- https://git.kernel.org/stable/c/3ec7437e9d11374105c2c4e47ae671537729d7e6
- https://git.kernel.org/stable/c/9c81bcc2c695e0082012a2a3d36a0eefaa51579c
- https://git.kernel.org/stable/c/9fca68c2512a362cad258e4df12a307bb2ee4b8e
- https://git.kernel.org/stable/c/b329fbcf075949a038045d8e9b86ae3d5bbd8a54

- https://git.kernel.org/stable/c/b427c2b05222db36d32ee141609de6128e9091bb
- https://security-tracker.debian.org/tracker/CVE-2026-43110
- https://access.redhat.com/security/cve/cve-2026-43110
- https://ubuntu.com/security/CVE-2026-43110
- https://bdu.fstec.ru/vul/2026-11323

3

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31478
BDU:2026-11321

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: 7.0 rc7
Ubuntu: 25.10
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.

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: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://git.kernel.org/stable/c/0e55f63dd08f09651d39e1b709a91705a8a0ddcb
- https://git.kernel.org/stable/c/4cb537ae4f37d7d0f617815ed4bed7173fb50861
- https://git.kernel.org/stable/c/6aef1765d6807e0f027cd87f6ac973eb0879a46d
- https://git.kernel.org/stable/c/70b4c414889492c522b6e4331562360f49be2361
- https://git.kernel.org/stable/c/80824c7e527b70cf9039534e60aff592e8f209d1
- https://git.kernel.org/stable/c/9a7166f0ef8cbb7bb48dd05e2471d995566003f5
- https://git.kernel.org/stable/c/c3a89e3ec1ccf64fa6a34e391e1581ebbcba8683
- https://ubuntu.com/security/CVE-2026-31478

- https://security-tracker.debian.org/tracker/CVE-2026-31478
- https://bdu.fstec.ru/vul/2026-11321

4

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46116
BDU:2026-11328

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

Уязвимый продукт: Linux: от 2.6.19 до 5.15.210
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
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.

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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/14acf9652e5690de3c7486c6db5fb8dafd0a32a3
- https://git.kernel.org/stable/c/26edb0a3c99f9d958c212be68b21f1221614dcf0
- https://git.kernel.org/stable/c/2c617848ae6e4f07a3e397f604208c293bbecacc
- https://git.kernel.org/stable/c/3943fcad7694a7d0b15aeabe7d3cc2a2eb8e92e8
- https://git.kernel.org/stable/c/4980162de555cb838f1a189ce7d2cbf5d2e7b050
- https://git.kernel.org/stable/c/6b4dc3181b4bfc5f5fc33ab33b1dc6e15759f4b6
- https://git.kernel.org/stable/c/a2e2d08fb070fab4947447171f1c4e3ca5a188e5

- https://git.kernel.org/stable/c/b4a53add2fa8f1b5aa17d4c5686c320785fab182
- https://security-tracker.debian.org/tracker/CVE-2026-46116
- https://access.redhat.com/security/cve/cve-2026-46116
- https://ubuntu.com/security/CVE-2026-46116
- https://bdu.fstec.ru/vul/2026-11328

5

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: BDU:2026-11285

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: -

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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2a00517db8de4be7df3d483b215c5544fb30a191
- https://ssd-disclosure.com/linux-bridge-stp-timer-use-after-free/
- https://bdu.fstec.ru/vul/2026-11285

6

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23240
BDU:2026-11240

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

Уязвимый продукт: Linux: от 5.3 до 6.12.74 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

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

Способ эксплуатации: Манипулирование 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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23240
- https://git.kernel.org/stable/c/a5de36d6cee74a92c1a21b260bc507e64bc451de
- https://git.kernel.org/stable/c/854cd32bc74fe573353095e90958490e4e4d641b
- https://git.kernel.org/stable/c/17153f154f80be2b47ebf52840f2d8f724eb2f3b
- https://git.kernel.org/linus/7bb09315f93dce6acc54bf59e5a95ba7365c2be4
- https://security-tracker.debian.org/tracker/CVE-2026-23240

- https://access.redhat.com/security/cve/CVE-2026-23240
- https://ubuntu.com/security/CVE-2026-23240
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://bdu.fstec.ru/vul/2026-11240

7

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-12326
BDU:2026-11241

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

Уязвимый продукт: Firefox: до 152.0.0
Thunderbird: до 152.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-12326
- https://security-tracker.debian.org/tracker/CVE-2026-12326
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-60/
- https://www.mozilla.org/security/advisories/mfsa2026-57/
- https://www.mozilla.org/security/advisories/mfsa2026-60/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-12326

- https://bdu.fstec.ru/vul/2026-11241

8

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-12293
BDU:2026-11243

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Firefox: до 152.0.0
Thunderbird: до 152.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-12293
- https://security-tracker.debian.org/tracker/CVE-2026-12293
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-60/
- https://www.mozilla.org/security/advisories/mfsa2026-57/
- https://www.mozilla.org/security/advisories/mfsa2026-60/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-12293

- https://bdu.fstec.ru/vul/2026-11243

9

Краткое описание: Повышение привилегий в TrueConf Server

Идентификатор уязвимости: CVE-2026-72529
BDU:2026-11246

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

Уязвимый продукт: TrueConf Server: от 5.5.0 до 5.5.5.10009

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: Не определено / Не определено

Ссылки на источник:

- https://securelist.ru/tr/head-mare-targets-trueconf-server-with-phantomcore/116557/
- https://trueconf.ru/blog/update/trueconf-server-security-update-june-2026
- https://ics-cert.kaspersky.ru/advisories/2026/08/07/otsutstvie-autentifikacii-dlyakriticheskoj-funkcii
- https://bdu.fstec.ru/vul/2026-11246

10

Краткое описание: Выполнение произвольного кода в TrueConf Server

Идентификатор уязвимости: CVE-2026-72530
BDU:2026-11247

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

Уязвимый продукт: TrueConf Server: от 5.5.0 до 5.5.5.10009

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: 9.0 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: Не определено / Не определено

Ссылки на источник:

- https://securelist.ru/tr/head-mare-targets-trueconf-server-with-phantomcore/116557/
- https://trueconf.ru/blog/update/trueconf-server-security-update-june-2026
- https://ics-cert.kaspersky.ru/advisories/2026/08/07/vyhod-iz-izolirovannoj-sredy
- https://bdu.fstec.ru/vul/2026-11247

11

Краткое описание: Повышение привилегий в MaxPatrol SIEM

Идентификатор уязвимости: BDU:2026-11249

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: MaxPatrol SIEM: 27.2.17150

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-27 / 2025-01-27

Ссылки на источник:

- https://ptsecurity.com/research/threatscape/PT-2026-21/
- https://bdu.fstec.ru/vul/2026-11249

12

Краткое описание: Внедрение кода в Firefox

Идентификатор уязвимости: CVE-2026-12316
BDU:2026-11250

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Firefox: до 152.0.0
Thunderbird: до 152.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

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: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-12316
- https://security-tracker.debian.org/tracker/CVE-2026-12316
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-60/
- https://www.mozilla.org/security/advisories/mfsa2026-57/
- https://www.mozilla.org/security/advisories/mfsa2026-60/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-12316

- https://bdu.fstec.ru/vul/2026-11250

13

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-12317
BDU:2026-11251

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

Уязвимый продукт: Firefox: до 152.0.0
Thunderbird: до 152.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-12317
- https://security-tracker.debian.org/tracker/CVE-2026-12317
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-60/
- https://www.mozilla.org/security/advisories/mfsa2026-57/
- https://www.mozilla.org/security/advisories/mfsa2026-60/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-12317

- https://bdu.fstec.ru/vul/2026-11251

14

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-14241
BDU:2026-11257

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox: до 152.0.4
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-14241
- https://security-tracker.debian.org/tracker/CVE-2026-14241
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-62/
- https://www.mozilla.org/security/advisories/mfsa2026-62/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-14241
- https://bdu.fstec.ru/vul/2026-11257

15

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31504
BDU:2026-11258

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.2 до 6.6.131
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-31504
- https://security-tracker.debian.org/tracker/CVE-2026-31504
- https://git.kernel.org/linus/42156f93d123436f2a27c468f18c966b7e5db796
- https://git.kernel.org/stable/c/1b4c03f8892d955385c202009af7485364731bb9
- https://git.kernel.org/stable/c/42156f93d123436f2a27c468f18c966b7e5db796
- https://git.kernel.org/stable/c/42cfd7898eeed290c9fb73f732af1f7d6b0a703e
- https://git.kernel.org/stable/c/654386baef228c2992dbf604c819e4c7c35fc71b

- https://git.kernel.org/stable/c/75fe6db23705a1d55160081f7b37db9665b1880b
- https://git.kernel.org/stable/c/ceccbfc6de720ad633519a226715989cfb065af1
- https://git.kernel.org/stable/c/d0c7cdc15fdf8c4f91aca1928e52295d175b6ec6
- https://git.kernel.org/stable/c/ee642b1962caa9aa231c01abbd58bc453ae6b66e
- https://github.com/4ab48b3f1ded2472/security-research/tree/CVE-2026-31504_cos/pocs/linux/kernelctf/CVE-2026-31504_cos
- https://lore.kernel.org/linux-cve-announce/2026042206-CVE-2026-31504-10f4@gregkh/T
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://access.redhat.com/security/cve/cve-2026-31504
- https://ubuntu.com/security/CVE-2026-31504
- https://bdu.fstec.ru/vul/2026-11258

16

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-6758
BDU:2026-11260

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Firefox: до 150.0
Thunderbird: до 150.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-6758
- https://security-tracker.debian.org/tracker/CVE-2026-6758
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-30/#CVE-2026-6758
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-33/#CVE-2026-6758
- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-6758
- https://bdu.fstec.ru/vul/2026-11260

17

Краткое описание: Получение конфиденциальной информации в Firefox

Идентификатор уязвимости: CVE-2026-6782
BDU:2026-11263

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

Уязвимый продукт: Firefox: до 150.0
Thunderbird: до 150.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-6782
- https://security-tracker.debian.org/tracker/CVE-2026-6782
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-30/#CVE-2026-6782
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-33/#CVE-2026-6782
- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-6782
- https://bdu.fstec.ru/vul/2026-11263

18

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-8952
BDU:2026-11265

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Firefox: до 151.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8952
- https://security-tracker.debian.org/tracker/CVE-2026-8952
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/#CVE-2026-8951
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8952
- https://bdu.fstec.ru/vul/2026-11265

19

Краткое описание: Внедрение кода в Firefox

Идентификатор уязвимости: CVE-2026-8963
BDU:2026-11267

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8963
- https://security-tracker.debian.org/tracker/CVE-2026-8963
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8963

- https://bdu.fstec.ru/vul/2026-11267

20

Краткое описание: Внедрение кода в Firefox

Идентификатор уязвимости: CVE-2026-8964
BDU:2026-11268

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8964
- https://security-tracker.debian.org/tracker/CVE-2026-8964
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8964

- https://bdu.fstec.ru/vul/2026-11268

21

Краткое описание: Получение конфиденциальной информации в Firefox

Идентификатор уязвимости: CVE-2026-8965
BDU:2026-11269

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8965
- https://security-tracker.debian.org/tracker/CVE-2026-8965
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8965

- https://bdu.fstec.ru/vul/2026-11269

22

Краткое описание: Получение конфиденциальной информации в Firefox

Идентификатор уязвимости: CVE-2026-8966
BDU:2026-11270

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8966
- https://security-tracker.debian.org/tracker/CVE-2026-8966
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8966

- https://bdu.fstec.ru/vul/2026-11270

23

Краткое описание: Получение конфиденциальной информации в Firefox

Идентификатор уязвимости: CVE-2026-8967
BDU:2026-11271

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8967
- https://security-tracker.debian.org/tracker/CVE-2026-8967
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8967

- https://bdu.fstec.ru/vul/2026-11271

24

Краткое описание: Внедрение кода в Firefox

Идентификатор уязвимости: CVE-2026-8969
BDU:2026-11272

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8969
- https://security-tracker.debian.org/tracker/CVE-2026-8969
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8969

- https://bdu.fstec.ru/vul/2026-11272

25

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-8972
BDU:2026-11274

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8972
- https://security-tracker.debian.org/tracker/CVE-2026-8972
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8972

- https://bdu.fstec.ru/vul/2026-11274

26

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-8973
BDU:2026-11275

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8973
- https://security-tracker.debian.org/tracker/CVE-2026-8973
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8973

- https://bdu.fstec.ru/vul/2026-11275

27

Краткое описание: Повышение привилегий в Linux

Идентификатор уязвимости: CVE-2026-64560
BDU:2026-11277

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

Уязвимый продукт: Linux: до 7.2-rc3
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026072908-CVE-2026-64560-3932@gregkh/
- https://git.kernel.org/stable/c/ad1cafa1bdaa71da85d71cac053838bbe97852b6
- https://git.kernel.org/stable/c/920f893f735e92ba3a1cd9256899a186b161928d
- https://github.com/villager1314/CVE-2026-64560-Analysis
- https://feedly.com/cve/CVE-2026-64560
- https://ubuntu.com/security/CVE-2026-64560
- https://access.redhat.com/security/cve/cve-2026-64560
- https://security-tracker.debian.org/tracker/CVE-2026-64560

- https://bdu.fstec.ru/vul/2026-11277

28

Краткое описание: Получение конфиденциальной информации в Traefik

Идентификатор уязвимости: CVE-2026-71324
BDU:2026-11278

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Traefik: от 3.7.0 до 3.7.9

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

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

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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://github.com/advisories/GHSA-3ccp-42pg-hgv6
- https://dailycve.com/traefik-cross-user-response-poisoning-cve-2026-71324-critical-dc-aug2026-1427/
- https://github.com/traefik/traefik/commit/04d36f28e4eae7535e96a6351dd9f7bfb48a30e7
- https://github.com/traefik/traefik/commit/0807b6d5dd1da8b2f7f4076ea2392b5437bf2ab0
- https://github.com/traefik/traefik/commit/94a7508817d180f0ab2f1eae93df48d4ab19ecce
- https://bdu.fstec.ru/vul/2026-11278

29

Краткое описание: Отказ в обслуживании в Clam Antivirus

Идентификатор уязвимости: BDU:2026-11282

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Clam Antivirus: от 1.5.0 до 1.5.3 включительно

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/Zer0SumGam3/clamav-zero-days/blob/main/01-zip-catalogue-double-free/README.md
- https://github.com/Zer0SumGam3/clamav-zero-days/blob/main/REPORT.MD
- https://bdu.fstec.ru/vul/2026-11282

30

Краткое описание: Выполнение произвольного кода в Clam Antivirus

Идентификатор уязвимости: BDU:2026-11284

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Clam Antivirus: 1.5.0 beta/RC

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/Zer0SumGam3/clamav-zero-days/blob/main/02-zip-index-desync-rce/README.md
- https://github.com/Zer0SumGam3/clamav-zero-days/blob/main/REPORT.MD
- https://bdu.fstec.ru/vul/2026-11284

31

Краткое описание: Перезапись произвольных файлов в Pillow

Идентификатор уязвимости: CVE-2026-59197
BDU:2026-11288

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Pillow: от 12.2.0 до 12.3.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Перезапись произвольных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/python-pillow/Pillow/commit/cce3bdb867c77a3420261ed1bfdb6b0787ec8fc1
- https://github.com/python-pillow/Pillow/pull/9695
- https://github.com/python-pillow/Pillow/releases/tag/12.3.0
- https://github.com/python-pillow/Pillow/security/advisories/GHSA-xj96-63gp-2gmr
- https://bdu.fstec.ru/vul/2026-11288

32

Краткое описание: Потеря целостности в Firefox

Идентификатор уязвимости: CVE-2026-8960
BDU:2026-11266

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

Уязвимый продукт: Firefox: до 151.0.0
Thunderbird: до 151.0.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Потеря целостности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8960
- https://security-tracker.debian.org/tracker/CVE-2026-8960
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-8960

- https://bdu.fstec.ru/vul/2026-11266

33

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-6768
BDU:2026-11262

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

Уязвимый продукт: Firefox: до 150.0
Thunderbird: до 150.0
Ubuntu: 22.04 LTS
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-6768
- https://security-tracker.debian.org/tracker/CVE-2026-6768
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-30/#CVE-2026-6768
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-33/#CVE-2026-6768
- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0805SE18HF
- https://ubuntu.com/security/CVE-2026-6768
- https://bdu.fstec.ru/vul/2026-11262

34

Краткое описание: Повышение привилегий в Windows File History Service

Идентификатор уязвимости: CVE-2026-57091
BDU:2026-11366

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 10.0.19044.7548
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: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57091
- https://bdu.fstec.ru/vul/2026-11366

35

Краткое описание: Выполнение произвольного кода в Windows SMB Server Network Transport Driver

Идентификатор уязвимости: CVE-2026-57089
BDU:2026-11365

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: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57089
- https://bdu.fstec.ru/vul/2026-11365

36

Краткое описание: Выполнение произвольного кода в Windows Server Network driver

Идентификатор уязвимости: CVE-2026-56188
BDU:2026-11364

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: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56188
- https://bdu.fstec.ru/vul/2026-11364

37

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-55947
BDU:2026-11363

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

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55947
- https://bdu.fstec.ru/vul/2026-11363

38

Краткое описание: Выполнение произвольного кода в Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central

Идентификатор уязвимости: CVE-2026-55944
BDU:2026-11362

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft Dynamics NAV 2018: до 11.0.50704.0

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: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55944
- https://bdu.fstec.ru/vul/2026-11362

39

Краткое описание: Повышение привилегий в Windows Hyper-V

Идентификатор уязвимости: CVE-2026-50680
BDU:2026-11361

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50680

- https://bdu.fstec.ru/vul/2026-11361

Краткое описание: Отказ в обслуживании в .NET

Идентификатор уязвимости: CVE-2026-50651
BDU:2026-11360

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

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

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

40 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50651
- https://bdu.fstec.ru/vul/2026-11360

41

Краткое описание: Повышение привилегий в Windows Runtime

Идентификатор уязвимости: CVE-2026-50457
BDU:2026-11359

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 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: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50457
- https://bdu.fstec.ru/vul/2026-11359

42

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2026-50328
BDU:2026-11357

Идентификатор программной ошибки: CWE-248 Необработанное исключение

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 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: 7.5 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50328
- https://bdu.fstec.ru/vul/2026-11357

43

Краткое описание: Выполнение произвольного кода в Windows NTFS

Идентификатор уязвимости: CVE-2026-50388
BDU:2026-11358

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 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: 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50388
- https://bdu.fstec.ru/vul/2026-11358

44

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-16411
BDU:2026-11353

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

Уязвимый продукт: Firefox: 152
Thunderbird: 152
Ubuntu: 22.04 LTS

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-68/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-71/
- https://ubuntu.com/security/CVE-2026-16411
- https://bdu.fstec.ru/vul/2026-11353

45

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-16360
BDU:2026-11354

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

Уязвимый продукт: Firefox: 152
Red Hat Enterprise Linux: 10
Firefox ESR: 140.12
Thunderbird: 152
Ubuntu: 22.04 LTS
Thunderbird ESR: 140.12

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-72/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-71/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-70/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-69/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-68/
- https://access.redhat.com/security/cve/cve-2026-16360

- https://ubuntu.com/security/CVE-2026-16360
- https://bdu.fstec.ru/vul/2026-11354

46

Краткое описание: Повышение привилегий в Linux

Идентификатор уязвимости: CVE-2026-64564
BDU:2026-11391

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.25 до 6.5 включительно
Red Hat Enterprise Linux: 10
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://matrix.tencent.com/en/2026/08/06/sctphantom-CVE-2026-64564
- https://git.kernel.org/stable/c/74e8f3e7114f0e26d1b2c4c048044db9fcc27603
- https://git.kernel.org/stable/c/85aca407c560aba81b5ce9d3d6cf94c74077d19b
- https://git.kernel.org/stable/c/9b2854f86f0b56e9027d68e7a3fc909d1a9b566f
- https://git.kernel.org/stable/c/d136b29bf91dd8e3161281b87de597b7311d9462
- https://git.kernel.org/stable/c/fedeb4468987bcaff85fe3061de5ae052d414740
- https://security-tracker.debian.org/tracker/CVE-2026-64564

- https://access.redhat.com/security/cve/cve-2026-64564
- https://ubuntu.com/security/CVE-2026-64564
- https://bdu.fstec.ru/vul/2026-11391

47

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64561
BDU:2026-11388

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.13 до 6.17 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://github.com/V4bel/Zapscape
- https://git.kernel.org/stable/c/0026dbb7de8ea76e97d6edf42fc3cc084564e2bf
- https://git.kernel.org/stable/c/2abd5287f08319fa35764566b15c6e22cb1068db
- https://git.kernel.org/stable/c/35e77467610c4a37cb0ff54ee56b85f73b1f5700
- https://git.kernel.org/stable/c/bce0d3c26e2c761a4bf43c8949f333fc7374eb2d
- https://git.kernel.org/stable/c/f3477a6a4164f15287444eda685b5f6405dbd1e5
- https://security-tracker.debian.org/tracker/CVE-2026-64561
- https://access.redhat.com/security/cve/cve-2026-64561

- https://ubuntu.com/security/CVE-2026-64561
- https://www.cve.org/CVERecord?id=CVE-2026-64561
- https://bdu.fstec.ru/vul/2026-11388

48

Краткое описание: Повышение привилегий в Microsoft Teams

Идентификатор уязвимости: CVE-2026-62896
BDU:2026-11461

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Microsoft Teams: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62896
- https://bdu.fstec.ru/vul/2026-11461

Краткое описание: Повышение привилегий в Azure Active Directory

Идентификатор уязвимости: CVE-2026-50481
BDU:2026-11462

Идентификатор программной ошибки: CWE-471 Изменение предположительно неизменяемых данных

Уязвимый продукт: Azure Active Directory: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50481
- https://bdu.fstec.ru/vul/2026-11462

50

Краткое описание: Выполнение произвольного кода в Azure Confidential Ledger

Идентификатор уязвимости: CVE-2026-68823
BDU:2026-11463

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: Azure Confidential Ledger: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68823/%22,
- https://bdu.fstec.ru/vul/2026-11463

51

Краткое описание: Получение конфиденциальной информации в Azure Logic Apps

Идентификатор уязвимости: CVE-2026-56161
BDU:2026-11464

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Azure Logic Apps: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56161
- https://bdu.fstec.ru/vul/2026-11464

52

Краткое описание: Выполнение произвольного кода в Azure Service Bus

Идентификатор уязвимости: CVE-2026-50515
BDU:2026-11465

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Azure Service Bus: -

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50515
- https://bdu.fstec.ru/vul/2026-11465

53

Краткое описание: Повышение привилегий в Azure SQL Database

Идентификатор уязвимости: CVE-2026-56162
BDU:2026-11466

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Azure SQL Database: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56162
- https://bdu.fstec.ru/vul/2026-11466

54

Краткое описание: Повышение привилегий в Azure SQL Managed Instance

Идентификатор уязвимости: CVE-2026-62836
BDU:2026-11467

Идентификатор программной ошибки: CWE-923 Некорректная проверка конечной точки для канала связи

Уязвимый продукт: Azure SQL Managed Instance: -

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62836
- https://bdu.fstec.ru/vul/2026-11467

55

Краткое описание: Повышение привилегий в Azure SRE Agent

Идентификатор уязвимости: CVE-2026-62830
BDU:2026-11468

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Azure SRE Agent: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62830
- https://bdu.fstec.ru/vul/2026-11468

56

Краткое описание: Выполнение произвольного кода в Microsoft Access

Идентификатор уязвимости: CVE-2026-64912
BDU:2026-11470

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

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

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: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64912
- https://bdu.fstec.ru/vul/2026-11470

57

Краткое описание: Повышение привилегий в Windows Installer

Идентификатор уязвимости: CVE-2026-70345
BDU:2026-11471

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70345
- https://bdu.fstec.ru/vul/2026-11471

58

Краткое описание: Повышение привилегий в .NET

Идентификатор уязвимости: CVE-2026-58641
BDU:2026-11486

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

Уязвимый продукт: .NET: от 9.0 до 9.0.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58641
- https://bdu.fstec.ru/vul/2026-11486

59

Краткое описание: Обход безопасности в Microsoft Office SharePoint

Идентификатор уязвимости: CVE-2026-70332
BDU:2026-11488

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

Уязвимый продукт: Microsoft SharePoint Online: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70332
- https://bdu.fstec.ru/vul/2026-11488

60

Краткое описание: Обход безопасности в Microsoft Teams

Идентификатор уязвимости: CVE-2026-62918
BDU:2026-11460

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Microsoft Teams: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62918
- https://bdu.fstec.ru/vul/2026-11460

61

Краткое описание: Повышение привилегий в Microsoft 365 Admin Center

Идентификатор уязвимости: CVE-2026-62873
BDU:2026-11469

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Microsoft 365 Admin Center: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62873
- https://bdu.fstec.ru/vul/2026-11469

62

Краткое описание: Повышение привилегий в Microsoft Teams

Идентификатор уязвимости: CVE-2026-65667
BDU:2026-11459

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Microsoft Teams: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65667
- https://bdu.fstec.ru/vul/2026-11459

63

Краткое описание: Повышение привилегий в Windows Kernel

Идентификатор уязвимости: CVE-2026-65773
BDU:2026-11458

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: 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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65773
- https://bdu.fstec.ru/vul/2026-11458

64

Краткое описание: Повышение привилегий в Windows DWM Core Library

Идентификатор уязвимости: CVE-2026-62894
BDU:2026-11457

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9115
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62894
- https://bdu.fstec.ru/vul/2026-11457

65

Краткое описание: Получение конфиденциальной информации в XWiki Platform

Идентификатор уязвимости: CVE-2026-48048
BDU:2026-11395

Идентификатор программной ошибки: CWE-359 Разглашение конфиденциальных данных (нарушение конфиденциальности)

Уязвимый продукт: XWiki Platform: до 18.0.0-rc-1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rh28-mqj4-8x59
- https://github.com/xwiki/xwiki-platform/commit/c4442716b02ffcdaa9d5e703b1db6203e36456fa
- https://jira.xwiki.org/browse/XWIKI-23875
- https://bdu.fstec.ru/vul/2026-11395

66

Краткое описание: Внедрение кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-17566
BDU:2026-11412

Идентификатор программной ошибки: CWE-115 Некорректная интерпретация входных данных

Уязвимый продукт: pgAdmin 4: до 9.17

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/HackSpeak/CVE-2026-17566
- https://github.com/pgadmin-org/pgadmin4/issues/10213
- https://github.com/pgadmin-org/pgadmin4/blob/REL-9_17/docs/en_US/release_notes_9_17.rst
- https://github.com/pgadmin-org/pgadmin4/commit/1496fabe28c9f825f6bac0f0d000d9d3276322c3
- https://bdu.fstec.ru/vul/2026-11412

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-64903
BDU:2026-11433

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

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 2016: до 16.0.5565.1001
Microsoft Office 2019: -
Microsoft Office 365: до 16.112.26081010

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

67

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В 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: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64903
- https://bdu.fstec.ru/vul/2026-11433

68

Краткое описание: Повышение привилегий в Windows Work Folder Service

Идентификатор уязвимости: CVE-2026-61349
BDU:2026-11434

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
Windows Server 2012 R2: до 6.3.9600.23338
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23338
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9115
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-61349
- https://bdu.fstec.ru/vul/2026-11434

69

Краткое описание: Повышение привилегий в Windows Kerberos

Идентификатор уязвимости: CVE-2026-62754
BDU:2026-11436

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
Windows 10 21H2: до 10.0.19044.7663
Windows 10 22H2: до 10.0.19045.7663
Windows 11 24H2: до 10.0.26000.9106
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 10.0.26100.33296
Windows Server 2025 (Server Core installation): до 10.0.26100.33296
Windows 11 25H2: до 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62754
- https://bdu.fstec.ru/vul/2026-11436

70

Краткое описание: Повышение привилегий в Windows Remote Access Connection Manager

Идентификатор уязвимости: CVE-2026-62783
BDU:2026-11437

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

Уязвимый продукт: 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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62783
- https://bdu.fstec.ru/vul/2026-11437

71

Краткое описание: Выполнение произвольного кода в Windows GDI+

Идентификатор уязвимости: CVE-2026-62822
BDU:2026-11440

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV: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: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62822
- https://bdu.fstec.ru/vul/2026-11440

72

Краткое описание: Выполнение произвольного кода в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-62823
BDU:2026-11441

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62823
- https://bdu.fstec.ru/vul/2026-11441

73

Краткое описание: Выполнение произвольного кода в Debian GNU/Linux

Идентификатор уязвимости: CVE-2026-64638
BDU:2026-11411

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

Уязвимый продукт: Debian GNU/Linux: 13
WordPress: от 4.7.0 до 4.7.34

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://github.com/imbas007/CVE-2026-64638-POC
- https://www.cve.org/CVERecord?id=CVE-2026-64638
- https://wordpress.org/news/2026/08/wordpress-7-0-3-release/
- https://security-tracker.debian.org/tracker/CVE-2026-64638
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-52p2-r8wf-jcrf
- https://github.com/HORKimhab/CVE-2026-64638
- https://bdu.fstec.ru/vul/2026-11411

74

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-68803
BDU:2026-11443

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.112.26081010
Microsoft Excel 2016: до 16.0.5565.1001
Microsoft Office LTSC 2024: до 16.112.26081010
Microsoft Office 2019: -
Microsoft Office 365: до 16.112.26081010

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68803
- https://bdu.fstec.ru/vul/2026-11443

75

Краткое описание: Выполнение произвольного кода в Microsoft Outlook

Идентификатор уязвимости: CVE-2026-70329
BDU:2026-11445

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

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70329
- https://bdu.fstec.ru/vul/2026-11445

76

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-62885
BDU:2026-11447

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62885
- https://bdu.fstec.ru/vul/2026-11447

77

Краткое описание: Повышение привилегий в Windows HTTP.sys

Идентификатор уязвимости: CVE-2026-62735
BDU:2026-11449

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62735
- https://bdu.fstec.ru/vul/2026-11449

78

Краткое описание: Повышение привилегий в Windows Installer

Идентификатор уязвимости: CVE-2026-70344
BDU:2026-11452

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70344
- https://bdu.fstec.ru/vul/2026-11452

79

Краткое описание: Повышение привилегий в Windows Kerberos

Идентификатор уязвимости: CVE-2026-62752
BDU:2026-11453

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62752
- https://bdu.fstec.ru/vul/2026-11453

80

Краткое описание: Повышение привилегий в Windows Device Association Service

Идентификатор уязвимости: CVE-2026-62747
BDU:2026-11456

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9115
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62747
- https://bdu.fstec.ru/vul/2026-11456

81

Краткое описание: Выполнение произвольного кода в Microsoft Local Security Authority Server

Идентификатор уязвимости: CVE-2026-62784
BDU:2026-11454

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV: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: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62784
- https://bdu.fstec.ru/vul/2026-11454

82

Краткое описание: Повышение привилегий в Desktop Window Manager

Идентификатор уязвимости: CVE-2026-65786
BDU:2026-11442

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 10.0.26000.9106
Windows Server 2016: до 10.0.14393.9418
Windows Server 2016 (Server Core installation): до 10.0.14393.9418
Windows Server 2019: до 10.0.17763.9115
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65786
- https://bdu.fstec.ru/vul/2026-11442

83

Краткое описание: Отказ в обслуживании в Adaptive Security Appliance

Идентификатор уязвимости: CVE-2026-20349
BDU:2026-11520

Идентификатор программной ошибки: CWE-244 Некорректная очистка динамической памяти перед ее освобождением (ревизия динамической памяти)

Уязвимый продукт: Adaptive Security Appliance: 9.24.1.11
Cisco Secure Firewall Threat Defense (FTD): 10.0.2

Категория уязвимого продукта: Средства защиты информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
- https://www.cisa.gov/news-events/alerts/2026/08/11/cisa-adds-three-known-exploited-vulnerabilities-catalog?_sp=66f416c1-1751-4a6d-ac96-6a016c2bdb43.1786603485565
- https://www.cybersecuritydive.com/news/cisco-firewall-vulnerabilities-vpn-crash/827688/
- https://socprime.com/blog/cve-2026-20349-actively-exploited-cisco-asa-and-ftd-flaw-enables-remote-dos/
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-11520

84

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-62700
BDU:2026-11634

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62700
- https://bdu.fstec.ru/vul/2026-11634

85

Краткое описание: Повышение привилегий в Windows Telephony Service

Идентификатор уязвимости: CVE-2026-62701
BDU:2026-11635

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62701
- https://bdu.fstec.ru/vul/2026-11635

86

Краткое описание: Выполнение произвольного кода в Windows SMBv3 Server

Идентификатор уязвимости: CVE-2026-62800
BDU:2026-11636

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV: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: 2026-08-12 / 2026-08-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62800
- https://bdu.fstec.ru/vul/2026-11636

87

Краткое описание: Повышение привилегий в Windows License Manager

Идентификатор уязвимости: CVE-2026-62777
BDU:2026-11637

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

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 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: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62777
- https://bdu.fstec.ru/vul/2026-11637

88

Краткое описание: Повышение привилегий в Windows Schannel

Идентификатор уязвимости: CVE-2026-62779
BDU:2026-11638

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62779
- https://bdu.fstec.ru/vul/2026-11638

89

Краткое описание: Выполнение произвольного кода в Application Testing Suite

Идентификатор уязвимости: CVE-2026-46924
BDU:2026-11644

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Application Testing Suite: 13.3.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11644

90

Краткое описание: Выполнение произвольного кода в Database Server

Идентификатор уязвимости: CVE-2026-60175
BDU:2026-11643

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Database Server: от 23.4.0 до 23.26.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11643

91

Краткое описание: Выполнение произвольного кода в Retail Integration Bus

Идентификатор уязвимости: CVE-2026-46983
BDU:2026-11645

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Retail Integration Bus: 16.0.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11645

92

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46875
BDU:2026-11657

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-11657

93

Краткое описание: Выполнение произвольного кода в Oracle Application Testing Suite

Идентификатор уязвимости: CVE-2026-35290
BDU:2026-11647

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Application Testing Suite: 13.3.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11647

94

Краткое описание: Выполнение произвольного кода в Oracle Application Testing Suite

Идентификатор уязвимости: CVE-2026-46876
BDU:2026-11648

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Application Testing Suite: 13.3.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11648

95

Краткое описание: Отказ в обслуживании в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46989
BDU:2026-11649

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.1 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L

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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11649

96

Краткое описание: Отказ в обслуживании в Database Server

Идентификатор уязвимости: CVE-2026-47040
BDU:2026-11650

Идентификатор программной ошибки: CWE-404 Некорректное освобождение ресурсов

Уязвимый продукт: Database Server: от 23.4.0 до 23.26.2 включительно

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

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11650

97

Краткое описание: Выполнение произвольного кода в E-Business Suite

Идентификатор уязвимости: CVE-2026-47031
BDU:2026-11651

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: E-Business Suite: от 12.2.3 до 12.2.15 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11651

98

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-47004
BDU:2026-11652

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11652

99

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46992
BDU:2026-11653

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11653

100

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46995
BDU:2026-11654

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11654

101

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46994
BDU:2026-11655

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11655

102

Краткое описание: Выполнение произвольного кода в Enterprise Manager Base Platform

Идентификатор уязвимости: CVE-2026-46855
BDU:2026-11656

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Enterprise Manager Base Platform: 13.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-11656

103

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-65775
BDU:2026-11632

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65775
- https://bdu.fstec.ru/vul/2026-11632

104

Краткое описание: Выполнение произвольного кода в Siebel CRM

Идентификатор уязвимости: CVE-2026-47036
BDU:2026-11646

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Siebel CRM: от 17.0 до 26.3 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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.oracle.com/security-alerts/cpujul2026.html
- https://bdu.fstec.ru/vul/2026-11646

105

Краткое описание: Повышение привилегий в Windows Installer

Идентификатор уязвимости: CVE-2026-65774
BDU:2026-11631

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65774
- https://bdu.fstec.ru/vul/2026-11631

106

Краткое описание: Повышение привилегий в Application Insights Profiler

Идентификатор уязвимости: CVE-2026-49163
BDU:2026-11621

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

Уязвимый продукт: Application Insights Profiler: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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: 2026-08-11 / 2026-08-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49163
- https://bdu.fstec.ru/vul/2026-11621

107

Краткое описание: Повышение привилегий в Windows Remote Access Connection Manager

Идентификатор уязвимости: CVE-2026-62758
BDU:2026-11629

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62758
- https://bdu.fstec.ru/vul/2026-11629

108

Краткое описание: Повышение привилегий в Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2026-61364
BDU:2026-11630

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

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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-61364
- https://bdu.fstec.ru/vul/2026-11630

109

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-22980
BDU:2026-11546

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.18 до 5.10.248
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-2026-22980
- https://security-tracker.debian.org/tracker/CVE-2026-22980
- https://git.kernel.org/linus/2857bd59feb63fcf40fe4baf55401baea6b4feb4
- https://git.kernel.org/stable/c/06600719d0f7a723811c45e4d51f5b742f345309
- https://git.kernel.org/stable/c/2857bd59feb63fcf40fe4baf55401baea6b4feb4
- https://git.kernel.org/stable/c/34eb22836e0cdba093baac66599d68c4cd245a9d
- https://git.kernel.org/stable/c/53f07d095e7e680c5e4569a55a019f2c0348cdc6
- https://git.kernel.org/stable/c/ba4811c8b433bfa681729ca42cc62b6034f223b0

- https://git.kernel.org/stable/c/ca97360860eb02e3ae4ba42c19b439a0fcecbf06
- https://git.kernel.org/stable/c/e8bfa2401d4c51eca6e48e9b33c798828ca9df61
- https://github.com/torvalds/linux/commit/53f07d095e7e680c5e4569a55a019f2c0348cdc6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-22980
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11546

110

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23025
BDU:2026-11547

Идентификатор программной ошибки: CWE-368 Состояние гонки, связанное с переключением контекста

Уязвимый продукт: Linux: от 6.1.57 до 6.1.162
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-2026-23025
- https://security-tracker.debian.org/tracker/CVE-2026-23025
- https://git.kernel.org/linus/038a102535eb49e10e93eafac54352fcc5d78847
- https://git.kernel.org/stable/c/038a102535eb49e10e93eafac54352fcc5d78847
- https://git.kernel.org/stable/c/3098f8f7c7b0686c74827aec42a2c45e69801ff8
- https://git.kernel.org/stable/c/4a04ff9cd816e7346fcc8126f00ed80481f6569d
- https://git.kernel.org/stable/c/68688fc4eab007834b4c2d740214423ba2a335a8
- https://git.kernel.org/stable/c/df63d31e9ae02e2f6cd96147779e4ed7cd0e75f6

- https://github.com/torvalds/linux/commit/3098f8f7c7b0686c74827aec42a2c45e69801ff8
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23025
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11547

111

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23083
BDU:2026-11564

Идентификатор программной ошибки: CWE-399 Уязвимости, связанные с управлением ресурсами

Уязвимый продукт: Linux: от 3.18 до 5.10.249
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: 7.8 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-2026-23083
- https://security-tracker.debian.org/tracker/CVE-2026-23083
- https://git.kernel.org/linus/7a9bc9e3f42391e4c187e099263cf7a1c4b69ff5
- https://git.kernel.org/stable/c/1cc98b8887cabb1808d2f4a37cd10a7be7574771
- https://git.kernel.org/stable/c/611ef4bd9c73d9e6d87bed57a635ff1fdd8c91ea
- https://git.kernel.org/stable/c/6e983789b7588ee59cbf303583546c043bad8e19
- https://git.kernel.org/stable/c/7a9bc9e3f42391e4c187e099263cf7a1c4b69ff5
- https://git.kernel.org/stable/c/9b75dff8446ec871030d8daf5a69e74f5fe8b956

- https://git.kernel.org/stable/c/b7db31a52c3862a1a32202a273a4c32e7f5f4823
- https://git.kernel.org/stable/c/c7498f9bc390479ccfad7c7f2332237ff4945b03
- https://github.com/torvalds/linux/commit/9b75dff8446ec871030d8daf5a69e74f5fe8b956
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23083
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11564

112

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23095
BDU:2026-11572

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

Уязвимый продукт: Linux: от 3.18 до 5.10.249
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-2026-23095
- https://security-tracker.debian.org/tracker/CVE-2026-23095
- https://git.kernel.org/linus/9a56796ad258786d3624eef5aefba394fc9bdded
- https://git.kernel.org/stable/c/380a82d36e37db49fd41ecc378c22fd29392e96a
- https://git.kernel.org/stable/c/536f5bbc322eb1e175bdd1ced22b236a951c4d8f
- https://git.kernel.org/stable/c/5437a279804ced8088cabb945dba88a26d828f8c
- https://git.kernel.org/stable/c/886f186328b718400dbf79e1bc8cbcbd710ab766
- https://git.kernel.org/stable/c/9a56796ad258786d3624eef5aefba394fc9bdded

- https://git.kernel.org/stable/c/ce569b389a5c78d64788a5ea94560e17fa574b35
- https://git.kernel.org/stable/c/f87b9b7a618c82e7465e872eb10e14c803871892
- https://github.com/torvalds/linux/commit/5437a279804ced8088cabb945dba88a26d828f8c
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23095
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11572

113

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23103
BDU:2026-11576

Идентификатор программной ошибки: CWE-667 Некорректная блокировка

Уязвимый продукт: Linux: от 4.17 до 5.10.249
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: 7.8 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-2026-23103
- https://security-tracker.debian.org/tracker/CVE-2026-23103
- https://git.kernel.org/linus/d3ba32162488283c0a4c5bedd8817aec91748802
- https://git.kernel.org/stable/c/04ba6de6eff61238e5397c14ac26a6578c7735a5
- https://git.kernel.org/stable/c/1f300c10d92c547c3a7d978e1212ff52f18256ed
- https://git.kernel.org/stable/c/3c149b662cbb202a450e81f938e702ba333864ad
- https://git.kernel.org/stable/c/6a81e2db096913d7e43aada1c350c1282e76db39
- https://git.kernel.org/stable/c/70feb16e3fbfb10b15de1396557c38e99f1ab8df

- https://git.kernel.org/stable/c/88f83e6c9cdb46b8c8ddd0ba01393362963cf589
- https://git.kernel.org/stable/c/d3ba32162488283c0a4c5bedd8817aec91748802
- https://github.com/torvalds/linux/commit/6a81e2db096913d7e43aada1c350c1282e76db39
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23103
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11576

114

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23169
BDU:2026-11595

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

Уязвимый продукт: Linux: от 6.13 до 6.18.9
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-2026-23169
- https://security-tracker.debian.org/tracker/CVE-2026-23169
- https://git.kernel.org/linus/e2a9eeb69f7d4ca4cf4c70463af77664fdb6ab1d
- https://git.kernel.org/stable/c/1f1b9523527df02685dde603f20ff6e603d8e4a1
- https://git.kernel.org/stable/c/338d40bab283da2639780ee3e458fb61f1567d8c
- https://git.kernel.org/stable/c/455e882192c9833f176f3fbbbb2f036b6c5bf555
- https://git.kernel.org/stable/c/51223bdd0f60b06cfc7f25885c4d4be917adba94

- https://git.kernel.org/stable/c/7896dbe990d56d5bb8097863b2645355633665eb
- https://git.kernel.org/stable/c/e2a9eeb69f7d4ca4cf4c70463af77664fdb6ab1d
- https://github.com/torvalds/linux/commit/1f1b9523527df02685dde603f20ff6e603d8e4a1
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23169
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11595

115

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23172
BDU:2026-11597

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

Уязвимый продукт: Linux: от 6.13 до 6.18.9
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: 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-2026-23172
- https://security-tracker.debian.org/tracker/CVE-2026-23172
- https://git.kernel.org/linus/f0813bcd2d9d97fdbdf2efb9532ab03ae92e99e6
- https://git.kernel.org/stable/c/2a0522f564acd34442652ea083091c329fa7c5d5
- https://git.kernel.org/stable/c/2c0fb0f60bc1545c52da61bc6bd4855c1e7814ba
- https://git.kernel.org/stable/c/af4b8577d0b388cc3d0039eb0cdd9ca5bbbc9276
- https://git.kernel.org/stable/c/f0813bcd2d9d97fdbdf2efb9532ab03ae92e99e6
- https://git.kernel.org/stable/c/f9747a7521a48afded5bff2faf1f2dcfff48c577

- https://github.com/torvalds/linux/commit/f0813bcd2d9d97fdbdf2efb9532ab03ae92e99e6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23172
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11597

116

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23178
BDU:2026-11599

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

Уязвимый продукт: Linux: от 6.7 до 6.12.70
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-2026-23178
- https://security-tracker.debian.org/tracker/CVE-2026-23178
- https://git.kernel.org/linus/2497ff38c530b1af0df5130ca9f5ab22c5e92f29
- https://git.kernel.org/stable/c/2124279f1f8c32c1646ce98e75a1a39b23b7db76
- https://git.kernel.org/stable/c/2497ff38c530b1af0df5130ca9f5ab22c5e92f29
- https://git.kernel.org/stable/c/786ec171788bdf9dda38789163f1b1fbb47f2d1e
- https://git.kernel.org/stable/c/cff3f619fd1cb40cdd89971df9001f075613d219

- https://git.kernel.org/stable/c/f9c9ad89d845f88a1509e9d672f65d234425fde9
- https://github.com/torvalds/linux/commit/2497ff38c530b1af0df5130ca9f5ab22c5e92f29
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23178
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11599

117

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23193
BDU:2026-11604

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.1 до 5.10.250
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-2026-23193
- https://security-tracker.debian.org/tracker/CVE-2026-23193
- https://git.kernel.org/linus/84dc6037390b8607c5551047d3970336cb51ba9a
- https://git.kernel.org/stable/c/11ebafffce31efc6abeb28c509017976fc49f1ca
- https://git.kernel.org/stable/c/2b64015550a13bcc72910be0565548d9a754d46d
- https://git.kernel.org/stable/c/41b86a9ec037bd3435d68dd3692f0891a207e7e7
- https://git.kernel.org/stable/c/4530f4e4d0e6a207110b0ffed0c911bca43531a4
- https://git.kernel.org/stable/c/84dc6037390b8607c5551047d3970336cb51ba9a

- https://git.kernel.org/stable/c/d8dbdc146e9e9a976931b78715be2e91299049f9
- https://git.kernel.org/stable/c/fd8b0900173307039d3a84644c2fee041a7ed4fb
- https://github.com/torvalds/linux/commit/4530f4e4d0e6a207110b0ffed0c911bca43531a4
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23193
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11604

118

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23198
BDU:2026-11605

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 4.4 до 5.10.250
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-2026-23198
- https://security-tracker.debian.org/tracker/CVE-2026-23198
- https://git.kernel.org/linus/b4d37cdb77a0015f51fee083598fa227cc07aaf1
- https://git.kernel.org/stable/c/2284bc168b148a17b5ca3b37b3d95c411f18a08d
- https://git.kernel.org/stable/c/4385b2f2843549bfb932e0dcf76bf4b065543a3c
- https://git.kernel.org/stable/c/6d14ba1e144e796b5fc81044f08cfba9024ca195
- https://git.kernel.org/stable/c/959a063e7f12524bc1871ad1f519787967bbcd45
- https://git.kernel.org/stable/c/b4d37cdb77a0015f51fee083598fa227cc07aaf1

- https://git.kernel.org/stable/c/b61f9b2fcf181451d0a319889478cc53c001123e
- https://git.kernel.org/stable/c/ff48c9312d042bfbe826ca675e98acc6c623211c
- https://github.com/torvalds/linux/commit/4385b2f2843549bfb932e0dcf76bf4b065543a3c
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23198
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11605

119

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23105
BDU:2026-11577

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

Уязвимый продукт: Linux: от 3.8 до 5.10.249
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-2026-23105
- https://security-tracker.debian.org/tracker/CVE-2026-23105
- https://git.kernel.org/linus/d837fbee92453fbb829f950c8e7cf76207d73f33
- https://git.kernel.org/stable/c/77f1afd0bb4d5da95236f6114e6d0dfcde187ff6
- https://git.kernel.org/stable/c/93b8635974fb050c43d07e35e5edfe6e685ca28a
- https://git.kernel.org/stable/c/abd9fc26ea577561a5ef6241a1b058755ffdad0c
- https://git.kernel.org/stable/c/b8c24cf5268fb3bfb8d16324c3dbb985f698c835
- https://git.kernel.org/stable/c/d837fbee92453fbb829f950c8e7cf76207d73f33

- https://git.kernel.org/stable/c/f27047abf7cac1b6f90c3ad60de21ef9f717c26d
- https://git.kernel.org/stable/c/fac2c67bb2bb732eae4283e45fc338af7e08c254
- https://github.com/torvalds/linux/commit/77f1afd0bb4d5da95236f6114e6d0dfcde187ff6
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23105
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11577

120

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23221
BDU:2026-11611

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.7 до 6.12.74
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-2026-23221
- https://security-tracker.debian.org/tracker/CVE-2026-23221
- https://git.kernel.org/linus/148891e95014b5dc5878acefa57f1940c281c431
- https://git.kernel.org/stable/c/148891e95014b5dc5878acefa57f1940c281c431
- https://git.kernel.org/stable/c/1d6bd6183e723a7b256ff34bbb5b498b5f4f2ec0
- https://git.kernel.org/stable/c/a2ae33e1c6361e960a4d00f7cf75d880b54f9528
- https://git.kernel.org/stable/c/b1983840287303e0dfb401b1b6cecc5ea7471e90
- https://git.kernel.org/stable/c/c424e72cfa67e7e1477035058a8a659f2c0ea637

- https://git.kernel.org/stable/c/c71dfb7833db7af652ee8f65011f14c97c47405d
- https://git.kernel.org/stable/c/dd8ba8c0c3f3916d4ee1e3a09da9cd5caff5d227
- https://github.com/torvalds/linux/commit/a2ae33e1c6361e960a4d00f7cf75d880b54f9528
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23221
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11611

121

Краткое описание: Повышение привилегий в Windows DHCP Client

Идентификатор уязвимости: CVE-2026-62755
BDU:2026-11628

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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 10.0.26000.9106
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 10.0.26100.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62755
- https://bdu.fstec.ru/vul/2026-11628

122

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23216
BDU:2026-11609

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 3.1 до 5.10.250
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-2026-23216
- https://security-tracker.debian.org/tracker/CVE-2026-23216
- https://git.kernel.org/linus/9411a89e9e7135cc459178fa77a3f1d6191ae903
- https://git.kernel.org/stable/c/275016a551ba1a068a3bd6171b18611726b67110
- https://git.kernel.org/stable/c/3835e49e146a4e6e7787b29465f1a23379b6ec44
- https://git.kernel.org/stable/c/48fe983e92de2c59d143fe38362ad17ba23ec7f3
- https://git.kernel.org/stable/c/73b487d44bf4f92942629d578381f89c326ff77f
- https://git.kernel.org/stable/c/8518f072fc92921418cd9ed4268dd4f3e9a8fd75

- https://git.kernel.org/stable/c/9411a89e9e7135cc459178fa77a3f1d6191ae903
- https://git.kernel.org/stable/c/ba684191437380a07b27666eb4e72748be1ea201
- https://github.com/torvalds/linux/commit/3835e49e146a4e6e7787b29465f1a23379b6ec44
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23216
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11609

123

Краткое описание: Повышение привилегий в Microsoft Purview eDiscovery

Идентификатор уязвимости: CVE-2026-65668
BDU:2026-11626

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Purview eDiscovery: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65668
- https://bdu.fstec.ru/vul/2026-11626

124

Краткое описание: Повышение привилегий в Copilot Cowork

Идентификатор уязвимости: CVE-2026-59118
BDU:2026-11625

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Microsoft Power Apps: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-59118
- https://bdu.fstec.ru/vul/2026-11625

125

Краткое описание: Повышение привилегий в Microsoft Entra Provisioning Service

Идентификатор уязвимости: CVE-2026-59115
BDU:2026-11623

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.]../...//[1.ков.]

Уязвимый продукт: Microsoft Entra Provisioning Service: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-59115
- https://bdu.fstec.ru/vul/2026-11623

126

Краткое описание: Повышение привилегий в Microsoft Planetary Computer Pro

Идентификатор уязвимости: CVE-2026-63508
BDU:2026-11624

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

Уязвимый продукт: Microsoft Planetary Computer Pro: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63508
- https://bdu.fstec.ru/vul/2026-11624

127

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-62880
BDU:2026-11617

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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/advisory/CVE-2026-62880
- https://bdu.fstec.ru/vul/2026-11617

128

Краткое описание: Выполнение произвольного кода в Windows Routing and Remote Access Service

Идентификатор уязвимости: CVE-2026-62819
BDU:2026-11616

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/advisory/CVE-2026-62819
- https://bdu.fstec.ru/vul/2026-11616

129

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-62877
BDU:2026-11615

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9418
Windows 10 1809: до 10.0.17763.9115
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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/advisory/CVE-2026-62877
- https://bdu.fstec.ru/vul/2026-11615

130

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23222
BDU:2026-11612

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 4.13 до 5.10.251
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-2026-23222
- https://security-tracker.debian.org/tracker/CVE-2026-23222
- https://git.kernel.org/linus/1562b1fb7e17c1b3addb15e125c718b2be7f5512
- https://git.kernel.org/stable/c/1562b1fb7e17c1b3addb15e125c718b2be7f5512
- https://git.kernel.org/stable/c/2ed27b5a1174351148c3adbfc0cd86d54072ba2e
- https://git.kernel.org/stable/c/31aff96a41ae6f1f1687c065607875a27c364da8
- https://git.kernel.org/stable/c/6edf8df4bd29f7bfd245b67b2c31d905f1cfc14b
- https://git.kernel.org/stable/c/79f95b51d4278044013672c27519ae88d07013d8

- https://git.kernel.org/stable/c/953c81941b0ad373674656b8767c00234ebf17ac
- https://git.kernel.org/stable/c/c184341920ed78b6466360ed7b45b8922586c38f
- https://git.kernel.org/stable/c/d1836c628cb72734eb5f7dfd4c996a9c18bba3ad
- https://github.com/torvalds/linux/commit/d1836c628cb72734eb5f7dfd4c996a9c18bba3ad
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://ubuntu.com/security/CVE-2026-23222
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11612