НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-08-13.1 | 13 августа 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2026-27690	SAP Approuter	Сетевой	SB	2026-07-14	✓
2	Критическая	CVE-2026-59083	Apache Tomcat	Сетевой	SB	2026-07-14	✓
3	Критическая	CVE-2026-59084	Apache Tomcat	Сетевой	OSI	2026-07-14	✓
4	Высокая	CVE-2022-50499	Linux	Локальный	ACE	2026-02-04	✓
5	Критическая	CVE-2026-39324	Rack::Session	Сетевой	DoS	2026-07-07	✓
6	Высокая	CVE-2026-40895	Node.js follow-redirects	Сетевой	OSI	2026-07-07	✓
7	Высокая	CVE-2022-50245	Linux	Локальный	ACE	2026-02-11	✓
8	Критическая	CVE-2026-20896	Gitea	Сетевой	ACE	2026-07-06	✓
9	Высокая	CVE-2026-27172	Apache Camel	Сетевой	ACE	2026-07-06	✓
10	Критическая	CVE-2026-40687	Exim	Сетевой	OAF	2026-07-07	✓
11	Высокая	CVE-2020-36049	Socket.IO	Сетевой	DoS	2026-07-07	✓
12	Критическая	CVE-2022-2421	Socket.IO	Сетевой	DoS	2026-07-07	✓
13	Критическая	CVE-2026-44963	Veeam Backup & Replication	Сетевой	ACE	2026-07-08	✓

14	Высокая	CVE-2026-11648	Google Chrome	Сетевой	ACE	2026-06-08	✓
15	Высокая	CVE-2026-11647	Google Chrome	Сетевой	SB	2026-06-08	✓
16	Высокая	CVE-2026-41722	VMware	Сетевой	XSS\CSS	2026-06-17	✓
17	Критическая	CVE-2026-0277	Prisma Access Agent	Смежная сеть	OSI	2026-07-10	✓
18	Высокая	CVE-2026-53571	Vite	Сетевой	OSI	2026-07-09	✓
19	Высокая	CVE-2026-56876	extract-zip	Сетевой	ACE	2026-07-10	✓
20	Высокая	CVE-2026-59873	node-tar	Сетевой	DoS	2026-07-10	✓
21	Высокая	CVE-2026-6896	Gitlab	Сетевой	XSS\CSS	2026-07-10	✓
22	Высокая	CVE-2026-43495	Linux	Смежная сеть	DoS	2026-02-09	✓
23	Высокая	CVE-2026-58253	NATS	Смежная сеть	PE	2026-07-14	✓
24	Высокая	CVE-2026-41724	VMware	Сетевой	XSS\CSS	2026-06-17	✓
25	Высокая	CVE-2026-41723	VMware	Сетевой	XSS\CSS	2026-06-17	✓
26	Критическая	CVE-2026-45495	Microsoft Edge	Сетевой	ACE	2026-07-13	✓
27	Высокая	CVE-2026-50413	Windows Runtime	Локальный	PE	2026-07-15	✓

28	Высокая	CVE-2026-49164	Windows Active Directory Domain Services	Сетевой	ACE	2026-07-15	✓
29	Высокая	CVE-2026-50649	.NET	Локальный	ACE	2026-07-15	✓
30	Высокая	CVE-2026-52943	Linux	Локальный	DoS	2026-07-15	✓
31	Высокая	CVE-2026-50510	GitHub Copilot	Локальный	ACE	2026-07-15	✓
32	Критическая	CVE-2026-50518	Windows DHCP Server	Сетевой	ACE	2026-07-15	✓
33	Критическая	CVE-2026-40047	Apache Camel	Сетевой	CI	2026-07-15	✓
34	Высокая	CVE-2026-58277	Microsoft SharePoint	Сетевой	PE	2026-07-15	✓
35	Высокая	CVE-2026-58617	M365 Copilot for iOS	Сетевой	PE	2026-07-15	✓
36	Высокая	CVE-2026-14191	WinRAR и UnRAR	Локальный	ACE	2026-07-15	✓
37	Высокая	CVE-2026-50474	Windows Remote Desktop Client	Сетевой	ACE	2026-07-16	✓
38	Высокая	CVE-2026-54121	Windows Active Directory Certificate Services	Сетевой	PE	2026-07-16	✓
39	Высокая	CVE-2026-56647	Windows Remote Access Service	Сетевой	PE	2026-07-16	✓
40	Высокая	CVE-2026-50306	Windows TCP/IP	Локальный	PE	2026-07-16	✓
41	Высокая	CVE-2026-50489	Windows Win32k	Локальный	PE	2026-07-15	✓
42	Критическая	CVE-2026-56699	Wazuh	Сетевой	ACE	2026-07-16	✓

43	Высокая	CVE-2026-50340	Windows Runtime	Сетевой	PE	2026-07-16	✓
44	Высокая	CVE-2026-49796	Windows GDI+	Локальный	ACE	2026-07-16	✓
45	Высокая	CVE-2026-54998	Microsoft Exchange Online	Сетевой	PE	2026-07-16	✓
46	Критическая	CVE-2026-57100	Microsoft Entra Provisioning Service	Сетевой	PE	2026-07-16	✓
47	Высокая	CVE-2026-57087	Windows Media Foundation	Сетевой	ACE	2026-07-16	✓
48	Высокая	CVE-2026-57090	Windows Media Foundation	Сетевой	ACE	2026-07-16	✓
49	Высокая	CVE-2026-54124	Windows Terminal	Локальный	ACE	2026-07-16	✓
50	Критическая	CVE-2026-49798	Windows	Локальный	PE	2026-07-16	✓
51	Критическая	CVE-2026-41106	Microsoft 365 Copilot	Сетевой	PE	2026-07-16	✓
52	Высокая	CVE-2026-58594	Windows Remote Desktop Client	Сетевой	ACE	2026-07-16	✓
53	Высокая	CVE-2026-57094	Windows Media Foundation	Сетевой	ACE	2026-07-16	✓
54	Высокая	CVE-2026-50670	Windows Win32k	Локальный	PE	2026-07-16	✓
55	Критическая	CVE-2026-50447	Windows Message Queuing Service	Сетевой	ACE	2026-07-16	✓
56	Высокая	CVE-2026-59835	FortiSandbox	Сетевой	SB	2026-07-16	✓
57	Высокая	CVE-2026-57821	Apache Fineract	Сетевой	CI	2026-07-16	✓

58	Критическая	CVE-2026-63087	Grafana OnCall	Сетевой	ACE	2026-07-17	✓
59	Высокая	CVE-2026-50385	Windows Runtime	Локальный	PE	2026-07-16	✓
60	Высокая	CVE-2026-46591	Apache Camel	Сетевой	ACE	2026-07-16	✓
61	Высокая	CVE-2026-50502	Windows Event Logging Service	Сетевой	ACE	2026-07-17	✓
62	Высокая	CVE-2026-50405	Windows Filtering Platform	Локальный	PE	2026-07-17	✓
63	Высокая	CVE-2026-42533	NGINX	Сетевой	ACE	2026-07-16	✓
64	Высокая	CVE-2026-50433	Windows Media	Локальный	PE	2026-07-17	✓
65	Высокая	CVE-2026-50373	Windows Search	Локальный	PE	2026-07-17	✓
66	Критическая	CVE-2026-58644	Microsoft SharePoint	Сетевой	ACE	2026-07-17	✓
67	Высокая	CVE-2026-50317	Windows	Локальный	PE	2026-07-16	✓
68	Высокая	CVE-2026-50329	Windows DWM Core Library	Локальный	PE	2026-07-16	✓
69	Высокая	CVE-2026-50314	Microsoft Office	Локальный	ACE	2026-07-16	✓
70	Высокая	CVE-2026-50471	Windows NTFS	Локальный	ACE	2026-07-20	✓
71	Высокая	CVE-2026-50469	Windows Projected File System	Локальный	PE	2026-07-20	✓
72	Критическая	CVE-2026-50380	Windows GDI+	Сетевой	ACE	2026-07-20	✓

73	Высокая	CVE-2026-10702	Firefox	Сетевой	ACE	2026-07-20	✓
74	Высокая	CVE-2026-50305	Windows Brokering File System	Локальный	PE	2026-07-20	✓
75	Высокая	CVE-2026-12484	Keras	Локальный	ACE	2026-07-20	✓
76	Высокая	CVE-2026-46590	Apache Camel	Сетевой	ACE	2026-07-20	✓
77	Критическая	CVE-2026-48203	Apache Camel	Сетевой	RLF	2026-07-20	✓
78	Высокая	CVE-2026-50363	Windows Push Notifications	Локальный	PE	2026-07-16	✓
79	Критическая	CVE-2026-47323	Apache Camel	Сетевой	ACE	2026-07-20	✓
80	Высокая	CVE-2026-50370	Windows DHCP Server Service	Смежная сеть	ACE	2026-07-20	✓
81	Высокая	CVE-2026-54128	Windows DHCP Client	Локальный	ACE	2026-07-17	✓
82	Высокая	CVE-2026-50382	Windows DirectX Graphics Kernel	Локальный	ACE	2026-07-17	✓
83	Критическая	CVE-2026-13585	ASUS System Control Interface	Сетевой	DoS	2026-07-20	✓
84	Высокая	CVE-2026-50326	Windows Unified Consent System	Локальный	PE	2026-07-17	✓
85	Высокая	CVE-2026-55130	Microsoft Word	Локальный	ACE	2026-07-20	✓
86	Высокая	CVE-2026-50378	Windows Key Guard	Локальный	PE	2026-07-20	✓
87	Высокая	CVE-2026-50313	Windows NTFS	Локальный	ACE	2026-07-17	✓

88	Высокая	CVE-2026-50461	Windows NTFS	Локальный	ACE	2026-07-17	✓
89	Высокая	CVE-2026-50301	Microsoft Office	Локальный	ACE	2026-07-17	✓
90	Высокая	CVE-2026-50417	Windows NTFS	Локальный	ACE	2026-07-17	✓
91	Высокая	CVE-2026-56156	Microsoft Excel	Локальный	ACE	2026-07-17	✓
92	Высокая	CVE-2026-50440	Windows Audio Service	Локальный	PE	2026-07-17	✓
93	Высокая	CVE-2026-39359	Wazuh	Сетевой	OSI	2026-07-20	✓
94	Высокая	CVE-2026-34150	Wazuh	Сетевой	DoS	2026-07-20	✓
95	Критическая	CVE-2026-50522	Microsoft SharePoint	Сетевой	ACE	2026-07-20	✓
96	Высокая	CVE-2026-54904	Concurrent Ruby	Сетевой	DoS	2026-07-20	✓
97	Высокая	CVE-2026-58532	Windows	Локальный	PE	2026-07-20	✓
98	Высокая	CVE-2026-49176	Windows WalletService	Локальный	PE	2026-07-20	✓
99	Высокая	CVE-2023-53187	Linux	Локальный	ACE	2026-07-20	✓
100	Высокая	CVE-2026-55033	Microsoft Office	Локальный	ACE	2026-07-17	✓
101	Высокая	CVE-2026-50369	Windows Remote Desktop Services	Сетевой	DoS	2026-07-21	✓
102	Высокая	CVE-2026-55833	Netty	Сетевой	DoS	2026-07-21	✓

103	Высокая	CVE-2026-50422	Windows NTFS	Локальный	PE	2026-07-16	✓
104	Высокая	CVE-2026-50667	Windows Common Log File System Driver	Локальный	PE	2026-07-16	✓
105	Высокая	CVE-2026-50484	Windows	Локальный	PE	2026-07-16	✓
106	Высокая	CVE-2026-50467	Microsoft Office	Локальный	ACE	2026-07-16	✓
107	Высокая	CVE-2026-50528	Microsoft .NET	Сетевой	OSI	2026-07-16	✓
108	Высокая	CVE-2026-50527	Microsoft .NET	Сетевой	DoS	2026-07-16	✓
109	Высокая	CVE-2026-50427	Windows Content Delivery Manager	Локальный	PE	2026-07-16	✓
110	Высокая	CVE-2026-58541	Microsoft DWM Core Library	Локальный	PE	2026-07-16	✓
111	Высокая	CVE-2026-50360	Windows SMB Server	Сетевой	PE	2026-07-16	✓
112	Высокая	CVE-2026-50407	Windows Resilient File System (ReFS)	Локальный	PE	2026-07-16	✓
113	Высокая	CVE-2026-50421	Windows Connected User Experiences and Telemetry	Локальный	PE	2026-07-16	✓
114	Высокая	CVE-2026-50458	Microsoft Brokering File System	Локальный	PE	2026-07-16	✓
115	Высокая	CVE-2026-50478	Windows	Локальный	PE	2026-07-15	✓
116	Высокая	CVE-2026-50477	Windows	Локальный	PE	2026-07-16	✓
117	Высокая	CVE-2026-50646	Microsoft .NET	Локальный	ACE	2026-07-16	✓

118	Высокая	CVE-2026-50355	Windows Active Directory Federation Services	Сетевой	DoS	2026-07-16	✓
119	Высокая	CVE-2026-59932	PhpSpreadsheet	Сетевой	DoS	2026-07-22	✓
120	Высокая	CVE-2026-59931	PhpSpreadsheet	Сетевой	RLF	2026-07-22	✓
121	Высокая	CVE-2026-58628	Windows Wireless Network Manager	Локальный	PE	2026-07-16	✓
122	Критическая	CVE-2026-63030	WordPress	Сетевой	ACE	2026-07-22	✓
123	Высокая	CVE-2025-40276	Linux	Смежная сеть	ACE	2026-07-21	✓
124	Высокая	CVE-2025-68195	Linux	Смежная сеть	ACE	2026-07-21	✓
125	Высокая	CVE-2026-55831	Netty	Сетевой	DoS	2026-07-15	✓
126	Критическая	CVE-2026-64620	FreeRDP	Сетевой	ACE	2026-07-22	✓
127	Критическая	CVE-2026-60137	WordPress	Сетевой	ACE	2026-07-22	✓
128	Высокая	CVE-2026-9973	Google Chrome	Сетевой	ACE	2026-06-08	✓
129	Высокая	CVE-2026-59933	PhpSpreadsheet	Сетевой	DoS	2026-07-22	✓
130	Высокая	CVE-2026-24291	Windows Accessibility Infrastructure	Локальный	PE	2026-03-13	✓

1

Краткое описание: Обход безопасности в SAP Approuter

Идентификатор уязвимости: CVE-2026-27690

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

Уязвимый продукт: SAP Approuter: до 20.10.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-14 / 2026-07-14

Ссылки на источник:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html
- https://me.sap.com/notes/3720138

2

Краткое описание: Обход безопасности в Apache Tomcat

Идентификатор уязвимости: CVE-2026-59083

Идентификатор программной ошибки: CWE-177 Некорректная обработка URL-кодировки (шестнадцатеричная кодировка)

Уязвимый продукт: Apache Tomcat: 9.0.13 - 11.0.23

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-14 / 2026-07-14

Ссылки на источник:

- https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.57
- https://github.com/apache/tomcat/commit/79466463f18cf57704513a5aaa93961bf14c9ef5
- https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.24
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.120
- https://github.com/apache/tomcat/commit/04e9ec3d32209faa26ca6c23ebd9ad514690aec0

3

Краткое описание: Получение конфиденциальной информации в Apache Tomcat

Идентификатор уязвимости: CVE-2026-59084

Идентификатор программной ошибки: CWE-1059 Неполная документация

Уязвимый продукт: Apache Tomcat: 9.0.13 - 11.0.23

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-14 / 2026-07-14

Ссылки на источник:

- https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.57
- https://github.com/apache/tomcat/commit/79466463f18cf57704513a5aaa93961bf14c9ef5
- https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.24
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.120
- https://github.com/apache/tomcat/commit/04e9ec3d32209faa26ca6c23ebd9ad514690aec0

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2022-50499
BDU:2026-09293

Идентификатор программной ошибки: CWE-665 Некорректная инициализация

Уязвимый продукт: Linux: от 4.19.77 до 4.19.269 включительно
Ubuntu: 22.04 LTS
Debian GNU/Linux: 11

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

4

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-04 / 2026-02-04

Ссылки на источник:

- https://git.kernel.org/stable/c/772892b29ac50c2c5e918fc80104aa6ede81d837
- https://git.kernel.org/stable/c/7dd5a68cdbbbe7fc67ba701cb52ba10d8ba149f8
- https://git.kernel.org/stable/c/acf984a3718c2458eb9e08b6714490a04f213c58
- https://git.kernel.org/stable/c/70bc51303871159796b55ba1a8f16637b46c2511
- https://git.kernel.org/stable/c/b21f62b49ee9c3e0216d685d9cfd6003e5727271
- https://git.kernel.org/stable/c/0588b12c418c3e4f927ced11f27b02ef4a5bfb07
- https://git.kernel.org/stable/c/123eddf92a114e03919942641d2c2b1f4ca56ea6
- https://git.kernel.org/stable/c/e9a78485b658361fab6a5547377be6c1af6f1b3d
- https://www.cve.org/CVERecord?id=CVE-2022-50499

- https://git.kernel.org/linus/6b0d0477fce747d4137aa65856318b55fba72198
- https://ubuntu.com/security/CVE-2022-50499
- https://security-tracker.debian.org/tracker/CVE-2022-50499
- https://lore.kernel.org/linux-cve-announce/2025100420-CVE-2022-50499-9f94@gregkh/
- https://bdu.fstec.ru/vul/2026-09293

5

Краткое описание: Отказ в обслуживании в Rack::Session

Идентификатор уязвимости: CVE-2026-39324
BDU:2026-09334

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: ПК СВ «Брест»: до 4.0.2
Rack::Session: от 2.0.0 до 2.1.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Ссылки на источник:

- https://github.com/rack/rack-session/commit/f43638cb3a4d15c3ecaf59e67a04b47fda08eeac
- https://github.com/rack/rack-session/security/advisories/GHSA-33qg-7wpp-89cq
- https://lk.astralinux.ru/
- https://nvd.nist.gov/vuln/detail/CVE-2026-39324
- https://security-tracker.debian.org/tracker/CVE-2026-39324
- https://bdu.fstec.ru/vul/2026-09334

6

Краткое описание: Получение конфиденциальной информации в Node.js follow-redirects

Идентификатор уязвимости: CVE-2026-40895
BDU:2026-09333

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

Уязвимый продукт: ПК СВ «Брест»: до 4.0.2
Follow Redirects: до 1.16.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/follow-redirects/follow-redirects/commit/844c4d302ac963d29bdb5dc1754ec7df3d70d7f9
- https://github.com/follow-redirects/follow-redirects/security/advisories/GHSA-r4q5-vmmm-2653
- https://lk.astralinux.ru/
- https://bdu.fstec.ru/vul/2026-09333

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2022-50245
BDU:2026-09309

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 4.6 до 4.9.336 включительно
Ubuntu: 22.04 LTS
Debian GNU/Linux: 11

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.

7

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2022-50245
- https://git.kernel.org/stable/c/2a6c75adf8192f07ddcdd4a1a13488c890a73919
- https://git.kernel.org/stable/c/2dfd60724d271a6ab99f93f40f38f2ced1ddbb87
- https://git.kernel.org/stable/c/a253dde0403a153075ffb254f6f7b2635e49e97a
- https://git.kernel.org/stable/c/311b488405ac45af46756b1c8f1d27007b68b07e
- https://git.kernel.org/stable/c/5ee850645e42f541ce1ea8130c2b27cc495f965c
- https://git.kernel.org/stable/c/2f5cc7fd73fd6253cc71214f0dd499cc62feb469
- https://git.kernel.org/stable/c/2ba06e57f933f0eac242e8b389433da1cc00d4d5
- https://git.kernel.org/stable/c/cb87af2c19c0993f6e21f75b963a5599c5a73e76

- https://git.kernel.org/linus/02d7d89f816951e0862147d751b1150d67aaebdd
- https://kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.337
- https://kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.303
- https://kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.270
- https://kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.4.229
- https://kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.163
- https://kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.86
- https://kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.0.16
- https://kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.1.2
- https://security-tracker.debian.org/tracker/CVE-2022-50245
- https://ubuntu.com/security/CVE-2022-50245
- https://lore.kernel.org/linux-cve-announce/2025091548-CVE-2022-50245-57e4@gregkh/
- https://bdu.fstec.ru/vul/2026-09309

8

Краткое описание: Выполнение произвольного кода в Gitea

Идентификатор уязвимости: CVE-2026-20896
BDU:2026-09304

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Gitea: до 1.26.3

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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://github.com/kaleth4/CVE-2026-20896
- https://github.com/go-gitea/gitea/security/advisories/GHSA-f75j-4cw6-rmx4
- https://blog.gitea.com/release-of-1.26.3-and-1.26.4/
- https://github.com/go-gitea/gitea/releases/tag/v1.26.3
- https://bdu.fstec.ru/vul/2026-09304

9

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2026-27172
BDU:2026-09300

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Camel: от 4.15.0 до 4.18.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-27172.html
- https://github.com/oscerd/CVE-2026-27172
- https://github.com/advisories/GHSA-5rc6-9qfp-8vwg
- https://bdu.fstec.ru/vul/2026-09300

10

Краткое описание: Перезапись произвольных файлов в Exim

Идентификатор уязвимости: CVE-2026-40687
BDU:2026-09402

Идентификатор программной ошибки: CWE-909 Отсутствует инициализация ресурса

Уязвимый продукт: Ubuntu: 26.04 LTS
exim: до 4.99.2
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Перезапись произвольных файлов

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

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

Ссылки на источник:

- https://code.exim.org/exim/exim/commit/68b963b9f75ca27b38e1c0f8c87037990199f505
- https://exim.org/static/doc/security/cve-2026-04.1/CVE2026-40687.assessment
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0611SE18HF
- https://www.openwall.com/lists/oss-security/2026/04/30/21
- https://security-tracker.debian.org/tracker/CVE-2026-40687
- https://ubuntu.com/security/CVE-2026-40687
- https://wiki.astralinux.ru/astra-linux-se48-bulletin-2026-0709SE48HF
- https://bdu.fstec.ru/vul/2026-09402

11

Краткое описание: Отказ в обслуживании в Socket.IO

Идентификатор уязвимости: CVE-2020-36049
BDU:2026-09401

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

Уязвимый продукт: ПК СВ «Брест»: до 4.0.2
Socket.IO: до 3.4.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://blog.caller.xyz/socketio-engineio-dos/
- https://github.com/bcaller/kill-engine-io
- https://github.com/socketio/socket.io-parser/commit/dcb942d24db97162ad16a67c2a0cf30875342d55
- https://lk.astralinux.ru/
- https://bdu.fstec.ru/vul/2026-09401

12

Краткое описание: Отказ в обслуживании в Socket.IO

Идентификатор уязвимости: CVE-2022-2421
BDU:2026-09400

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

Уязвимый продукт: ПК СВ «Брест»: до 4.0.2
Socket.IO: от 4.0.0 до 4.2.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://csirt.divd.nl/cves/CVE-2022-2421/
- https://lk.astralinux.ru/
- https://bdu.fstec.ru/vul/2026-09400

13

Краткое описание: Выполнение произвольного кода в Veeam Backup & Replication

Идентификатор уязвимости: CVE-2026-44963
BDU:2026-09346

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Veeam Backup & Replication: до 12.3.2.4854

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

Ссылки на источник:

- https://www.veeam.com/kb4869
- https://blog.securelayer7.net/cve-2026-44963-veeam-backup-authenticated-rce-binaryformatter-bypass/
- https://bdu.fstec.ru/vul/2026-09346

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11648
BDU:2026-09349

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103
Microsoft Edge: до 149.0.4022.62

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11648
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11648
- https://security-tracker.debian.org/tracker/CVE-2026-11648
- https://bdu.fstec.ru/vul/2026-09349

15

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11647
BDU:2026-09350

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11647
- https://security-tracker.debian.org/tracker/CVE-2026-11647
- https://bdu.fstec.ru/vul/2026-09350

16

Краткое описание: Межсайтовый скриптинг в VMware

Идентификатор уязвимости: CVE-2026-41722
BDU:2026-09507

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

Уязвимый продукт: VMware Cloud Foundation: до 8.18.7
VMware Aria Operations: до 8.18.7
VMware Telco Cloud Platform: до KB443138
VMware vSphere Foundation: до 9.1.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-17 / 2026-06-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37513
- https://bdu.fstec.ru/vul/2026-09507

17

Краткое описание: Получение конфиденциальной информации в Prisma Access Agent

Идентификатор уязвимости: CVE-2026-0277
BDU:2026-09553

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Prisma Access Agent: до 26.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-10 / 2026-07-10

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0277
- https://bdu.fstec.ru/vul/2026-09553

18

Краткое описание: Получение конфиденциальной информации в Vite

Идентификатор уязвимости: CVE-2026-53571
BDU:2026-09524

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

Уязвимый продукт: Vite: от 6.0.0 до 6.4.3
Vite+: до 0.1.24

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/vitejs/vite/security/advisories/GHSA-fx2h-pf6j-xcff
- https://feedly.com/cve/CVE-2026-53571
- https://github.com/TazmiDev/CVE-2026-53571
- https://bdu.fstec.ru/vul/2026-09524

19

Краткое описание: Выполнение произвольного кода в extract-zip

Идентификатор уязвимости: CVE-2026-56876
BDU:2026-09561

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

Уязвимый продукт: extract-zip: до 2.0.1 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-10 / 2026-07-10

Ссылки на источник:

- https://github.com/ziad626/CVE-2026-56876-POC
- https://github.com/max-mapper/extract-zip
- https://github.com/ziad626/extract-zip-security-research/security/advisories/GHSA-x7jf-2287-qcpf
- https://bdu.fstec.ru/vul/2026-09561

20

Краткое описание: Отказ в обслуживании в node-tar

Идентификатор уязвимости: CVE-2026-59873
BDU:2026-09563

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

Уязвимый продукт: node-tar: до 7.5.19

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-07-10 / 2026-07-10

Ссылки на источник:

- https://github.com/isaacs/node-tar/commit/2812e9338665659b183aa7226518c307044957d3
- https://github.com/isaacs/node-tar/releases/tag/v7.5.19
- https://github.com/isaacs/node-tar/security/advisories/GHSA-23hp-3jrh-7fpw
- https://bdu.fstec.ru/vul/2026-09563

21

Краткое описание: Межсайтовый скриптинг в Gitlab

Идентификатор уязвимости: CVE-2026-6896
BDU:2026-09564

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

Уязвимый продукт: Gitlab: от 19.1.0 до 19.1.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.7 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-10 / 2026-07-10

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-2-released/
- https://bdu.fstec.ru/vul/2026-09564

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43495
BDU:2026-09580

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 5.19 до 7.1-rc3
Debian GNU/Linux: 13
openSUSE Tumbleweed: -

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.

22 **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: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://security-tracker.debian.org/tracker/CVE-2026-43495
- https://www.cybersecurity-help.cz/vdb/vulns/132125/
- https://lore.kernel.org/linux-cve-announce/2026052155-CVE-2026-43495-9b17@gregkh/T/#u
- https://git.kernel.org/stable/c/0e7c074cfcd9bd93765505f9eb8b42f03ed2a744
- https://git.kernel.org/stable/c/2b56d7903ab804481f5233a259d5f341e9fd513c
- https://git.kernel.org/stable/c/9855e063e063158cc5bded576382599dc3133202
- https://git.kernel.org/stable/c/f94450ce5053b36002995b72d1fa1db3bb08c5bf
- https://www.suse.com/security/cve/CVE-2026-43495.html
- https://lore.kernel.org/linux-cve-announce/2026052155-CVE-2026-43495-9b17@gregkh/

- https://access.redhat.com/security/cve/cve-2026-43495
- https://bdu.fstec.ru/vul/2026-09580

23

Краткое описание: Повышение привилегий в NATS

Идентификатор уязвимости: CVE-2026-58253
BDU:2026-09678

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: NATS: до 2.14.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-14 / 2026-07-14

Ссылки на источник:

- https://github.com/nats-io/nats-server/security/advisories/GHSA-38x3-76xf-cq45
- https://github.com/nats-io/nats-server/releases/tag/v2.11.16
- https://github.com/nats-io/nats-server/releases/tag/v2.12.7
- https://github.com/nats-io/nats-server/releases/tag/v2.14.0
- https://dailycve.com/nats-server-improper-authentication-cve-2026-58253-medium-dc-jul2026-926/
- https://bdu.fstec.ru/vul/2026-09678

24

Краткое описание: Межсайтовый скриптинг в VMware

Идентификатор уязвимости: CVE-2026-41724
BDU:2026-09761

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

Уязвимый продукт: VMware Cloud Foundation: до 8.18.7
VMware Aria Operations: до 8.18.7
VMware Telco Cloud Platform: до KB443138

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-17 / 2026-06-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37513
- https://bdu.fstec.ru/vul/2026-09761

25

Краткое описание: Межсайтовый скриптинг в VMware

Идентификатор уязвимости: CVE-2026-41723
BDU:2026-09762

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

Уязвимый продукт: VMware Cloud Foundation: до 8.18.7
VMware Aria Operations: до 8.18.7
VMware Telco Cloud Platform: до KB443138
VMware vSphere Foundation: до 9.1.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-17 / 2026-06-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37513
- https://bdu.fstec.ru/vul/2026-09762

26

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-45495
BDU:2026-09757

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

Уязвимый продукт: Microsoft Edge: до 148.0.3967.70

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-13 / 2026-07-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45495
- https://bdu.fstec.ru/vul/2026-09757

27

Краткое описание: Повышение привилегий в Windows Runtime

Идентификатор уязвимости: CVE-2026-50413
BDU:2026-09803

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50413
- https://bdu.fstec.ru/vul/2026-09803

28

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

Идентификатор уязвимости: CVE-2026-49164
BDU:2026-09806

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49164
- https://bdu.fstec.ru/vul/2026-09806

Краткое описание: Выполнение произвольного кода в .NET

Идентификатор уязвимости: CVE-2026-50649
BDU:2026-09808

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: .NET: от 9.0 до 9.0.18
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: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50649
- https://bdu.fstec.ru/vul/2026-09808

30

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-52943
BDU:2026-09715

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

Уязвимый продукт: Linux: от 6.7 до 6.12.93
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8
Amazon Linux 2: Kernel-5.4 Extra
Amazon Linux 2023: -

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://git.kernel.org/linus/98d0912e9f841e5529a5b89a972805f34cb1c69d
- https://git.kernel.org/stable/c/2e0e74c59b2761a414d9f48d7bee1e45220b2427
- https://git.kernel.org/stable/c/474d6c771d798bca84f0a140b611e36743511e18
- https://git.kernel.org/stable/c/8dbed691e43a50903658130bde0fcb5abc425b37
- https://git.kernel.org/stable/c/96a4713ae041cc85e712bac682cd2e644004d6c6
- https://git.kernel.org/stable/c/98d0912e9f841e5529a5b89a972805f34cb1c69d

- https://git.kernel.org/stable/c/9b40bdc2a3298225dffab8158208a0d8c6300578
- https://git.kernel.org/stable/c/ceafb893b12f23331dcc5ff9587e643c3a40ee9f
- https://git.kernel.org/stable/c/fd470f0a97b8e9a125f520265d2f3b088ffb5b8a
- https://github.com/vn-lazyming/CVE-2026-52943
- https://lore.kernel.org/linux-cve-announce/2026062406-CVE-2026-52943-88f7@gregkh/T/#u
- https://nvd.nist.gov/vuln/detail/CVE-2026-52943
- https://security-tracker.debian.org/tracker/CVE-2026-52943
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0706SE18HF
- https://ubuntu.com/security/CVE-2026-52943
- https://security-tracker.debian.org/tracker/CVE-2026-52943
- https://explore.alas.aws.amazon.com/CVE-2026-52943.html
- https://access.redhat.com/security/cve/cve-2026-52943
- https://bdu.fstec.ru/vul/2026-09715

31

Краткое описание: Выполнение произвольного кода в GitHub Copilot

Идентификатор уязвимости: CVE-2026-50510
BDU:2026-09723

Идентификатор программной ошибки: CWE-641 Некорректные ограничения для имен фалов и ресурсов

Уязвимый продукт: GitHub Copilot Plugin for JetBrains IDEs: до 1.13.0-251

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50510
- https://bdu.fstec.ru/vul/2026-09723

32

Краткое описание: Выполнение произвольного кода в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-50518
BDU:2026-09725

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows Server 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50518
- https://bdu.fstec.ru/vul/2026-09725

33

Краткое описание: Внедрение кода в Apache Camel

Идентификатор уязвимости: CVE-2026-40047
BDU:2026-09731

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: Camel: от 4.15.0 до 4.18.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-40047.html
- https://www.openwall.com/lists/oss-security/2026/07/05/2
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-55881
- https://github.com/oscerd/CVE-2026-40047
- https://bdu.fstec.ru/vul/2026-09731

34

Краткое описание: Повышение привилегий в Microsoft SharePoint

Идентификатор уязвимости: CVE-2026-58277
BDU:2026-09729

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение 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: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58277
- https://bdu.fstec.ru/vul/2026-09729

35

Краткое описание: Повышение привилегий в M365 Copilot for iOS

Идентификатор уязвимости: CVE-2026-58617
BDU:2026-09738

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft 365 Copilot: -

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: 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: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58617
- https://bdu.fstec.ru/vul/2026-09738

36

Краткое описание: Выполнение произвольного кода в WinRAR и UnRAR

Идентификатор уязвимости: CVE-2026-14191
BDU:2026-09733

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: UnRAR: до 7.23
WinRAR: до 7.23

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://www.rarlab.com/download.htm
- https://www.securin.io/zero-days/cve-2026-14191-winrar-unrar-rar5-recovery-volume-rev-out-of-bounds-heap-write-in-recvolumes5-readheader
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-54451
- https://github.com/HORKimhab/CVE-2026-14191
- https://bdu.fstec.ru/vul/2026-09733

37

Краткое описание: Выполнение произвольного кода в Windows Remote Desktop Client

Идентификатор уязвимости: CVE-2026-50474
BDU:2026-09850

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50474
- https://bdu.fstec.ru/vul/2026-09850

38

Краткое описание: Повышение привилегий в Windows Active Directory Certificate Services

Идентификатор уязвимости: CVE-2026-54121
BDU:2026-09854

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54121
- https://bdu.fstec.ru/vul/2026-09854

39

Краткое описание: Повышение привилегий в Windows Remote Access Service

Идентификатор уязвимости: CVE-2026-56647
BDU:2026-09863

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19044.7548
Windows 11 24H2: до 10.0.26100.8875
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26100.8875
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: 8.8 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56647
- https://bdu.fstec.ru/vul/2026-09863

40

Краткое описание: Повышение привилегий в Windows TCP/IP

Идентификатор уязвимости: CVE-2026-50306
BDU:2026-09826

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50306
- https://bdu.fstec.ru/vul/2026-09826

41

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-50489
BDU:2026-09815

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50489
- https://bdu.fstec.ru/vul/2026-09815

42

Краткое описание: Выполнение произвольного кода в Wazuh

Идентификатор уязвимости: CVE-2026-56699
BDU:2026-09828

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Wazuh: до 5.0.0-beta3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-ff9g-85jq-r3g3
- https://bdu.fstec.ru/vul/2026-09828

43

Краткое описание: Повышение привилегий в Windows Runtime

Идентификатор уязвимости: CVE-2026-50340
BDU:2026-09866

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование 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: 8.5 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50340
- https://bdu.fstec.ru/vul/2026-09866

44

Краткое описание: Выполнение произвольного кода в Windows GDI+

Идентификатор уязвимости: CVE-2026-49796
BDU:2026-09889

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49796
- https://bdu.fstec.ru/vul/2026-09889

45

Краткое описание: Повышение привилегий в Microsoft Exchange Online

Идентификатор уязвимости: CVE-2026-54998
BDU:2026-09887

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Microsoft Exchange Online: -

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54998
- https://bdu.fstec.ru/vul/2026-09887

46

Краткое описание: Повышение привилегий в Microsoft Entra Provisioning Service

Идентификатор уязвимости: CVE-2026-57100
BDU:2026-09886

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

Уязвимый продукт: Microsoft Entra Provisioning Service: -

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: 9.9 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57100
- https://bdu.fstec.ru/vul/2026-09886

47

Краткое описание: Выполнение произвольного кода в Windows Media Foundation

Идентификатор уязвимости: CVE-2026-57087
BDU:2026-09884

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57087
- https://bdu.fstec.ru/vul/2026-09884

48

Краткое описание: Выполнение произвольного кода в Windows Media Foundation

Идентификатор уязвимости: CVE-2026-57090
BDU:2026-09883

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57090
- https://bdu.fstec.ru/vul/2026-09883

Краткое описание: Выполнение произвольного кода в Windows Terminal

Идентификатор уязвимости: CVE-2026-54124
BDU:2026-09984

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

Уязвимый продукт: Windows Terminal: до 1.24.11321.0
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 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

49

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54124
- https://bdu.fstec.ru/vul/2026-09984

50

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-49798
BDU:2026-09980

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49798
- https://bdu.fstec.ru/vul/2026-09980

51

Краткое описание: Повышение привилегий в Microsoft 365 Copilot

Идентификатор уязвимости: CVE-2026-41106
BDU:2026-09975

Идентификатор программной ошибки: CWE-601 Перенаправление на небезопасный сайт ("открытое перенаправление")

Уязвимый продукт: Microsoft 365 Copilot: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Повышение привилегий

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

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41106
- https://bdu.fstec.ru/vul/2026-09975

52

Краткое описание: Выполнение произвольного кода в Windows Remote Desktop Client

Идентификатор уязвимости: CVE-2026-58594
BDU:2026-09969

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58594
- https://bdu.fstec.ru/vul/2026-09969

53

Краткое описание: Выполнение произвольного кода в Windows Media Foundation

Идентификатор уязвимости: CVE-2026-57094
BDU:2026-09966

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57094
- https://bdu.fstec.ru/vul/2026-09966

54

Краткое описание: Повышение привилегий в Windows Win32k

Идентификатор уязвимости: CVE-2026-50670
BDU:2026-10039

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50670

- https://bdu.fstec.ru/vul/2026-10039

55

Краткое описание: Выполнение произвольного кода в Windows Message Queuing Service

Идентификатор уязвимости: CVE-2026-50447
BDU:2026-09960

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50447
- https://bdu.fstec.ru/vul/2026-09960

56

Краткое описание: Обход безопасности в FortiSandbox

Идентификатор уязвимости: CVE-2026-59835
BDU:2026-09917

Идентификатор программной ошибки: CWE-668 Возможность несанкционированного доступа к ресурсу

Уязвимый продукт: FortiSandbox: от 4.4.3 до 4.4.9

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-145
- https://bdu.fstec.ru/vul/2026-09917

57

Краткое описание: Внедрение кода в Apache Fineract

Идентификатор уязвимости: CVE-2026-57821
BDU:2026-09905

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

Уязвимый продукт: Fineract: до 1.15.0

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: 8.1 AV:N/AC:L/PR:L/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: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://github.com/tc4dy/CVE-2026-57821-PoC-Exploit
- https://lists.apache.org/thread/rj5vwh3z2xcvsf0rqwj8kokpbrxkhq4n
- https://bdu.fstec.ru/vul/2026-09905

58

Краткое описание: Выполнение произвольного кода в Grafana OnCall

Идентификатор уязвимости: CVE-2026-63087
BDU:2026-09904

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

Уязвимый продукт: Grafana OnCall: до 1.16.11 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://www.vulncheck.com/advisories/grafana-oncall-unauthenticated-token-hijack-via-plugin-install-endpoint
- https://github.com/geo-chen/oss/blob/main/oncall.md
- https://bdu.fstec.ru/vul/2026-09904

59

Краткое описание: Повышение привилегий в Windows Runtime

Идентификатор уязвимости: CVE-2026-50385
BDU:2026-09961

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50385
- https://bdu.fstec.ru/vul/2026-09961

60

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2026-46591
BDU:2026-09895

Идентификатор программной ошибки: CWE-1001 Модели программных сбоев (вторичный кластер): использование некорректного API

Уязвимый продукт: Camel: от 4.10.0 до 4.14.8

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-46591.html
- https://github.com/oscerd/CVE-2026-46591
- https://github.com/apache/camel/commit/7881d949c40befcc602016dcce25a2fb38d070ce
- https://github.com/apache/camel/pull/23258
- https://issues.apache.org/jira/browse/CAMEL-23528
- https://bdu.fstec.ru/vul/2026-09895

61

Краткое описание: Выполнение произвольного кода в Windows Event Logging Service

Идентификатор уязвимости: CVE-2026-50502
BDU:2026-09944

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50502
- https://bdu.fstec.ru/vul/2026-09944

62

Краткое описание: Повышение привилегий в Windows Filtering Platform

Идентификатор уязвимости: CVE-2026-50405
BDU:2026-09941

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

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: 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: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50405
- https://bdu.fstec.ru/vul/2026-09941

63

Краткое описание: Выполнение произвольного кода в NGINX

Идентификатор уязвимости: CVE-2026-42533
BDU:2026-09927

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

Уязвимый продукт: NGINX Ingress Controller: от 5.0.0 до 5.5.3
NGINX Instance Manager: от 2.17.0 до 2.22.1 включительно
NGINX Plus: от R33 до R36 P7
NGINX Open Source: от 1.30.0 до 1.30.4
NGINX Gateway Fabric: от 2.0.0 до 2.6.7
F5 WAF for NGINX: от 5.9.0 до 5.13.3 включительно
NGINX App Protect WAF: от 4.11.0 до 4.16.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://my.f5.com/manage/s/article/K000162097
- https://1275.ru/vulnerability/vyshel-patch-dlya-nginx-tri-kriticheskie-uyazvimosti-zakryty-v-versiyah-1-30-4-i-1-31-3_32184
- https://github.com/0xCyberstan/CVE-2026-42533-Config-Scanner
- https://bdu.fstec.ru/vul/2026-09927

64

Краткое описание: Повышение привилегий в Windows Media

Идентификатор уязвимости: CVE-2026-50433
BDU:2026-09937

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50433
- https://bdu.fstec.ru/vul/2026-09937

65

Краткое описание: Повышение привилегий в Windows Search

Идентификатор уязвимости: CVE-2026-50373
BDU:2026-09933

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

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: 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: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50373

- https://bdu.fstec.ru/vul/2026-09933

66

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint

Идентификатор уязвимости: CVE-2026-58644
BDU:2026-09928

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20384
Microsoft SharePoint Enterprise Server 2016: до 16.0.5556.1005
Microsoft SharePoint Server 2019: до 16.0.10417.20153

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: 9.8 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: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-58644
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-09928

67

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-50317
BDU:2026-10120

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50317
- https://bdu.fstec.ru/vul/2026-10120

68

Краткое описание: Повышение привилегий в Windows DWM Core Library

Идентификатор уязвимости: CVE-2026-50329
BDU:2026-10119

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50329

- https://bdu.fstec.ru/vul/2026-10119

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-50314
BDU:2026-10118

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

69

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50314
- https://bdu.fstec.ru/vul/2026-10118

70

Краткое описание: Выполнение произвольного кода в Windows NTFS

Идентификатор уязвимости: CVE-2026-50471
BDU:2026-10115

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows 10 21H2: до 10.0.19044.7548
Windows 10 22H2: до 10.0.19045.7548
Windows 11 23H2: до 10.0.22631.7376
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 2022 (Server Core installation): до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158
Windows 11 25H2: до 10.0.26100.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50471
- https://bdu.fstec.ru/vul/2026-10115

71

Краткое описание: Повышение привилегий в Windows Projected File System

Идентификатор уязвимости: CVE-2026-50469
BDU:2026-10114

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

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 ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50469

- https://bdu.fstec.ru/vul/2026-10114

72

Краткое описание: Выполнение произвольного кода в Windows GDI+

Идентификатор уязвимости: CVE-2026-50380
BDU:2026-10112

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50380
- https://bdu.fstec.ru/vul/2026-10112

73

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-10702
BDU:2026-10106

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

Уязвимый продукт: Firefox: до 151.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-54/
- https://github.com/NebuSec/CyberMeowfia/tree/main/IonStack/CVE-2026-10702
- https://www.sentinelone.com/vulnerability-database/cve-2026-10702/
- https://bdu.fstec.ru/vul/2026-10106

74

Краткое описание: Повышение привилегий в Windows Brokering File System

Идентификатор уязвимости: CVE-2026-50305
BDU:2026-10108

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50305
- https://bdu.fstec.ru/vul/2026-10108

75

Краткое описание: Выполнение произвольного кода в Keras

Идентификатор уязвимости: CVE-2026-12484
BDU:2026-10105

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Keras: 3.15.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://huntr.com/bounties/ab14df49-13b5-4442-b754-3189430bfa28
- https://bdu.fstec.ru/vul/2026-10105

76

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2026-46590
BDU:2026-10104

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Camel: от 4.18.0 до 4.18.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://www.sentinelone.com/vulnerability-database/cve-2026-46590/
- https://camel.apache.org/security/CVE-2026-46590.html
- https://github.com/oscerd/CVE-2026-46590
- https://bdu.fstec.ru/vul/2026-10104

77

Краткое описание: Чтение локальных файлов в Apache Camel

Идентификатор уязвимости: CVE-2026-48203
BDU:2026-10103

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

Уязвимый продукт: Camel: от 4.19.0 до 4.21.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Чтение локальных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://camel.apache.org/security/CVE-2026-48203.html
- https://github.com/oscerd/CVE-2026-48203
- https://bdu.fstec.ru/vul/2026-10103

78

Краткое описание: Повышение привилегий в Windows Push Notifications

Идентификатор уязвимости: CVE-2026-50363
BDU:2026-10122

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50363
- https://bdu.fstec.ru/vul/2026-10122

79

Краткое описание: Выполнение произвольного кода в Apache Camel

Идентификатор уязвимости: CVE-2026-47323
BDU:2026-10102

Идентификатор программной ошибки: CWE-791 Неполная фильтрация специальных элементов

Уязвимый продукт: Camel: от 3.18.0 до 4.14.6
OpenShift Serverless: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://github.com/advisories/GHSA-8364-hfqj-pwm6
- https://github.com/oscerd/CVE-2026-47323
- https://camel.apache.org/security/CVE-2026-47323.html
- https://access.redhat.com/security/cve/cve-2026-47323
- https://bdu.fstec.ru/vul/2026-10102

80

Краткое описание: Выполнение произвольного кода в Windows DHCP Server Service

Идентификатор уязвимости: CVE-2026-50370
BDU:2026-10110

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9339
Windows 10 1809: до 10.0.17763.9020
Windows Server 2012: до 6.2.9200.26226
Windows Server 2012 R2: до 6.3.9600.23291
Windows Server 2012 (Server Core installation): до 6.2.9200.26226
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23291
Windows Server 2016: до 10.0.14393.9339
Windows Server 2016 (Server Core installation): до 10.0.14393.9339
Windows Server 2019: до 10.0.17763.9020
Windows Server 2019 (Server Core installation): до 10.0.17763.9020
Windows Server 2022: до 10.0.20348.5386
Windows Server 2025: до 10.0.26100.33158
Windows Server 2025 (Server Core installation): до 10.0.26100.33158

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50370
- https://bdu.fstec.ru/vul/2026-10110

81

Краткое описание: Выполнение произвольного кода в Windows DHCP Client

Идентификатор уязвимости: CVE-2026-54128
BDU:2026-10124

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54128
- https://bdu.fstec.ru/vul/2026-10124

82

Краткое описание: Выполнение произвольного кода в Windows DirectX Graphics Kernel

Идентификатор уязвимости: CVE-2026-50382
BDU:2026-10142

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50382

- https://bdu.fstec.ru/vul/2026-10142

83

Краткое описание: Отказ в обслуживании в ASUS System Control Interface

Идентификатор уязвимости: CVE-2026-13585
BDU:2026-10101

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

Уязвимый продукт: System Control Interface: до 1.1.40.0
Business Manager: до 3.0.38.0 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

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: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://github.com/416rehman/asus-bsitf-0-day-poc
- https://www.asus.com/security-advisory/
- https://ift.tt/35rJvPn
- https://bdu.fstec.ru/vul/2026-10101

84

Краткое описание: Повышение привилегий в Windows Unified Consent System

Идентификатор уязвимости: CVE-2026-50326
BDU:2026-10155

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50326
- https://bdu.fstec.ru/vul/2026-10155

85

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-55130
BDU:2026-10151

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55130
- https://bdu.fstec.ru/vul/2026-10151

86

Краткое описание: Повышение привилегий в Windows Key Guard

Идентификатор уязвимости: CVE-2026-50378
BDU:2026-10150

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

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 сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50378
- https://bdu.fstec.ru/vul/2026-10150

87

Краткое описание: Выполнение произвольного кода в Windows NTFS

Идентификатор уязвимости: CVE-2026-50313
BDU:2026-10146

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50313
- https://bdu.fstec.ru/vul/2026-10146

88

Краткое описание: Выполнение произвольного кода в Windows NTFS

Идентификатор уязвимости: CVE-2026-50461
BDU:2026-10144

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50461
- https://bdu.fstec.ru/vul/2026-10144

89

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-50301
BDU:2026-10140

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50301
- https://bdu.fstec.ru/vul/2026-10140

90

Краткое описание: Выполнение произвольного кода в Windows NTFS

Идентификатор уязвимости: CVE-2026-50417
BDU:2026-10139

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50417
- https://bdu.fstec.ru/vul/2026-10139

91

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-56156
BDU:2026-10137

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56156
- https://bdu.fstec.ru/vul/2026-10137

Краткое описание: Повышение привилегий в Windows Audio Service

Идентификатор уязвимости: CVE-2026-50440
BDU:2026-10125

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8875
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

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50440
- https://bdu.fstec.ru/vul/2026-10125

93

Краткое описание: Получение конфиденциальной информации в Wazuh

Идентификатор уязвимости: CVE-2026-39359
BDU:2026-10095

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

Уязвимый продукт: Wazuh: от 4.11.0 до 4.14.5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-6q95-fcwc-4h44
- https://github.com/CVEProject/cvelistV5/blob/main/cves/2026/39xxx/CVE-2026-39359.json
- https://osv.dev/vulnerability/CVE-2026-39359
- https://bdu.fstec.ru/vul/2026-10095

94

Краткое описание: Отказ в обслуживании в Wazuh

Идентификатор уязвимости: CVE-2026-34150
BDU:2026-10087

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

Уязвимый продукт: Wazuh: от 1.0.0 до 4.14.5

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-rvr9-89q8-w883
- https://bdu.fstec.ru/vul/2026-10087

95

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint

Идентификатор уязвимости: CVE-2026-50522
BDU:2026-10084

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
- https://fedisecfeeds.github.io/
- https://www.zerodayinitiative.com/advisories/ZDI-26-412/
- https://www.kaspersky.ru/blog/update-microsoft-patch-tuesday-july-2026-570-bugs/42283/
- https://bdu.fstec.ru/vul/2026-10084

96

Краткое описание: Отказ в обслуживании в Concurrent Ruby

Идентификатор уязвимости: CVE-2026-54904
BDU:2026-10083

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

Уязвимый продукт: Concurrent Ruby: до 1.3.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://github.com/ruby-concurrency/concurrent-ruby/security/advisories/GHSA-h8w8-99g7-qmvj
- https://github.com/CVEProject/cvelistV5/blob/main/cves/2026/54xxx/CVE-2026-54904.json
- https://bdu.fstec.ru/vul/2026-10083

97

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-58532
BDU:2026-10074

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58532
- https://core-jmp.org/2026/07/cve-2026-58532-tcpip-sys-integer-overflow/
- https://bdu.fstec.ru/vul/2026-10074

98

Краткое описание: Повышение привилегий в Windows WalletService

Идентификатор уязвимости: CVE-2026-49176
BDU:2026-10073

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: 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: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49176
- https://github.com/DavidCarliez/CVE-2026-49176_LPE_POC
- https://bdu.fstec.ru/vul/2026-10073

99

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2023-53187
BDU:2026-10185

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

Уязвимый продукт: Linux: от 5.15.128 до 5.16
Debian GNU/Linux: 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: 2026-07-20 / 2026-07-20

Ссылки на источник:

- https://git.kernel.org/stable/c/7569c4294ba6ff9f194635b14876198f8a687c4a
- https://git.kernel.org/stable/c/6297644db23f77c02ae7961cc542d162629ae2c4
- https://www.cve.org/CVERecord?id=CVE-2023-53187
- https://git.kernel.org/linus/0657b20c5a76c938612f8409735a8830d257866e
- https://lore.kernel.org/linux-cve-announce/2025091557-CVE-2023-53187-fb77@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2023-53187
- https://bdu.fstec.ru/vul/2026-10185

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-55033
BDU:2026-10184

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

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

Категория уязвимого продукта: Прикладное программное обеспечение

100

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-17 / 2026-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55033
- https://bdu.fstec.ru/vul/2026-10184

101

Краткое описание: Отказ в обслуживании в Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2026-50369
BDU:2026-10168

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 сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50369
- https://github.com/syxlox/CVE-2026-50369
- https://bdu.fstec.ru/vul/2026-10168

102

Краткое описание: Отказ в обслуживании в Netty

Идентификатор уязвимости: CVE-2026-55833
BDU:2026-10163

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

Уязвимый продукт: Netty: от 4.1.0.Final до 4.1.136.Final

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/netty/netty/security/advisories/GHSA-mvh2-crg5-v77c
- https://github.com/netty/netty/commit/5b68c61f37aa4a3045cba624cbea239655c9003b
- https://github.com/netty/netty/commit/bb2ff68a1fb71cb4b0eb9a9e17b66c52aff680c6
- https://github.com/netty/netty/releases/tag/netty-4.1.136.Final
- https://github.com/netty/netty/releases/tag/netty-4.2.16.Final
- https://bdu.fstec.ru/vul/2026-10163

103

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-50422
BDU:2026-10320

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50422
- https://bdu.fstec.ru/vul/2026-10320

104

Краткое описание: Повышение привилегий в Windows Common Log File System Driver

Идентификатор уязвимости: CVE-2026-50667
BDU:2026-10319

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50667
- https://bdu.fstec.ru/vul/2026-10319

105

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-50484
BDU:2026-10318

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50484

- https://bdu.fstec.ru/vul/2026-10318

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-50467
BDU:2026-10315

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.111.26071215
Microsoft Office LTSC 2024: до 16.111.26071215
Microsoft Office 2016: до 16.0.5561.1000
Microsoft Office 2019: -
Microsoft Office 365: до 16.111.26071215

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

106 **Последствия эксплуатации:** Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50467
- https://bdu.fstec.ru/vul/2026-10315

Краткое описание: Получение конфиденциальной информации в Microsoft .NET

Идентификатор уязвимости: CVE-2026-50528
BDU:2026-10310

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: .NET: от 8.0 до 8.0.29
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: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50526
- https://bdu.fstec.ru/vul/2026-10310

108

Краткое описание: Отказ в обслуживании в Microsoft .NET

Идентификатор уязвимости: CVE-2026-50527
BDU:2026-10309

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: .NET: от 8.0 до 8.0.29
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50527
- https://bdu.fstec.ru/vul/2026-10309

109

Краткое описание: Повышение привилегий в Windows Content Delivery Manager

Идентификатор уязвимости: CVE-2026-50427
BDU:2026-10314

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50427
- https://bdu.fstec.ru/vul/2026-10314

110

Краткое описание: Повышение привилегий в Microsoft DWM Core Library

Идентификатор уязвимости: CVE-2026-58541
BDU:2026-10327

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58541
- https://bdu.fstec.ru/vul/2026-10327

111

Краткое описание: Повышение привилегий в Windows SMB Server

Идентификатор уязвимости: CVE-2026-50360
BDU:2026-10339

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: 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 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: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50360
- https://bdu.fstec.ru/vul/2026-10339

112

Краткое описание: Повышение привилегий в Windows Resilient File System (ReFS)

Идентификатор уязвимости: CVE-2026-50407
BDU:2026-10344

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50407
- https://bdu.fstec.ru/vul/2026-10344

113

Краткое описание: Повышение привилегий в Windows Connected User Experiences and Telemetry

Идентификатор уязвимости: CVE-2026-50421
BDU:2026-10345

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50421
- https://bdu.fstec.ru/vul/2026-10345

114

Краткое описание: Повышение привилегий в Microsoft Brokering File System

Идентификатор уязвимости: CVE-2026-50458
BDU:2026-10348

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50458
- https://bdu.fstec.ru/vul/2026-10348

115

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-50478
BDU:2026-10351

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50478

- https://bdu.fstec.ru/vul/2026-10351

116

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-50477
BDU:2026-10352

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50477
- https://bdu.fstec.ru/vul/2026-10352

Краткое описание: Выполнение произвольного кода в Microsoft .NET

Идентификатор уязвимости: CVE-2026-50646
BDU:2026-10353

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: .NET: от 9.0 до 9.0.18
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

117

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50646
- https://bdu.fstec.ru/vul/2026-10353

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

Идентификатор уязвимости: CVE-2026-50355
BDU:2026-10354

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
Microsoft .NET Framework 3.5: до 3.0.30729.8978
Microsoft .NET Framework 4.6.2: до 4.7.4143.0
Microsoft .NET Framework 4.7: до 4.7.4143.0
Microsoft .NET Framework 4.7.1: до 4.7.4143.0
Microsoft .NET Framework 4.7.2: до 3.0.30729.9067
Microsoft .NET Framework 4.8: до 3.0.30729.9067
Microsoft .NET Framework 4.8.1: до 4.8.9339.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

118

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50355
- https://bdu.fstec.ru/vul/2026-10354

119

Краткое описание: Отказ в обслуживании в PhpSpreadsheet

Идентификатор уязвимости: CVE-2026-59932
BDU:2026-10358

Идентификатор программной ошибки: CWE-409 Некорректная обработка данных с высокой степенью сжатия (увеличение объема данных)

Уязвимый продукт: PhpSpreadsheet: до 1.30.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/PHPOffice/PhpSpreadsheet/security/advisories/GHSA-2mrg-gjxq-2gvr
- github.com/PHPOffice/PhpSpreadsheet/releases
- https://bdu.fstec.ru/vul/2026-10358

120

Краткое описание: Чтение локальных файлов в PhpSpreadsheet

Идентификатор уязвимости: CVE-2026-59931
BDU:2026-10359

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

Уязвимый продукт: PhpSpreadsheet: до 1.30.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/PHPOffice/PhpSpreadsheet/security/advisories/GHSA-6hq5-7373-42rg
- github.com/PHPOffice/PhpSpreadsheet/releases
- https://bdu.fstec.ru/vul/2026-10359

121

Краткое описание: Повышение привилегий в Windows Wireless Network Manager

Идентификатор уязвимости: CVE-2026-58628
BDU:2026-10329

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

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 10.0.26100.8875
Windows 11 26H1: до 10.0.28000.2525

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58628
- https://bdu.fstec.ru/vul/2026-10329

122

Краткое описание: Выполнение произвольного кода в WordPress

Идентификатор уязвимости: CVE-2026-63030
BDU:2026-10241

Идентификатор программной ошибки: CWE-436 Конфликт интерпретации

Уязвимый продукт: WordPress: до 7.1 beta2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Анализ целевого объекта

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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.picussecurity.com/resource/blog/cve-2026-63030-and-cve-2026-60137-wp2shell-wordpress-rce-explained
- https://github.com/Bhanunamikaze/WP2Shell-CVE-2026-63030-POC
- https://github.com/Colere-Sys/wp2shell-poc
- https://github.com/mrmtwoj/Fix-CVE-2026-60137-CVE-2026-63030-in-wordpress
- https://isc.sans.edu/diary/WordPress+Exploitation+Underway+CVE202663030/33168
- https://www.rapid7.com/blog/post/etr-cve-2026-63030-wp2shell-a-critical-remote-code-execution-vulnerability-in-wordpress-core/
- https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- https://flawfence.com/blog/en/wp2shell-wordpress-rce-vulnerability-cve-2026-63030/
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
- https://www.vulncheck.com/blog/wp2shell
- https://bdu.fstec.ru/vul/2026-10241

123

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2025-40276
BDU:2026-10221

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

Уязвимый продукт: Linux: от 6.10 до 6.17.8 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2025-40276
- https://git.kernel.org/stable/c/7a12f9c96d06b145562f76ffb20369b4692f0911
- https://git.kernel.org/linus/576c930e5e7dcb937648490611a83f1bf0171048
- https://kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.17.9
- https://lore.kernel.org/linux-cve-announce/2025120717-CVE-2025-40276-6558@gregkh/
- https://security-tracker.debian.org/tracker/CVE-2025-40276
- https://bdu.fstec.ru/vul/2026-10221

124

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2025-68195
BDU:2026-10222

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

Уязвимый продукт: Linux: от 6.12.58 до 6.13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2025-68195
- https://git.kernel.org/stable/c/4c6b56a76478bd1ab609827c571905386c11d308
- https://git.kernel.org/linus/f1fdffe0afea02ba783acfe815b6a60e7180df40
- https://lore.kernel.org/linux-cve-announce/2025121636-CVE-2025-68195-98fc@gregkh/
- https://bdu.fstec.ru/vul/2026-10222

125

Краткое описание: Отказ в обслуживании в Netty

Идентификатор уязвимости: CVE-2026-55831
BDU:2026-10237

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

Уязвимый продукт: Netty: от 4.1.0.Final до 4.1.136.Final

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-15 / 2026-07-15

Ссылки на источник:

- https://github.com/netty/netty/releases/tag/netty-4.1.136.Final
- https://github.com/netty/netty/releases#release-netty-4.2.13.Final
- https://github.com/netty/netty/security/advisories/GHSA-6jqx-86gh-f27w
- https://bdu.fstec.ru/vul/2026-10237

126

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-64620
BDU:2026-10238

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

Уязвимый продукт: FreeRDP: до 3.28.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-pjqx-v446-x7fc
- https://github.com/FreeRDP/FreeRDP/releases#release-3.28.0
- https://bdu.fstec.ru/vul/2026-10238

127

Краткое описание: Выполнение произвольного кода в WordPress

Идентификатор уязвимости: CVE-2026-60137
BDU:2026-10242

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

Уязвимый продукт: WordPress: от 6.8.0 до 6.8.6

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.picussecurity.com/resource/blog/cve-2026-63030-and-cve-2026-60137-wp2shell-wordpress-rce-explained
- https://github.com/Bhanunamikaze/WP2Shell-CVE-2026-63030-POC
- https://github.com/Colere-Sys/wp2shell-poc
- https://github.com/mrmtwoj/Fix-CVE-2026-60137-CVE-2026-63030-in-wordpress
- https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- https://flawfence.com/blog/en/wp2shell-wordpress-rce-vulnerability-cve-2026-63030/
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf
- https://www.vulncheck.com/blog/wp2shell
- https://bdu.fstec.ru/vul/2026-10242

128

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-9973
BDU:2026-10243

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9973
- https://github.com/jaf0rk/CVE-2026-9973-exploit
- https://bdu.fstec.ru/vul/2026-10243

129

Краткое описание: Отказ в обслуживании в PhpSpreadsheet

Идентификатор уязвимости: CVE-2026-59933
BDU:2026-10360

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

Уязвимый продукт: PhpSpreadsheet: до 1.30.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/PHPOffice/PhpSpreadsheet/security/advisories/GHSA-xh5m-36r6-47m3
- github.com/PHPOffice/PhpSpreadsheet/releases
- https://bdu.fstec.ru/vul/2026-10360

130

Краткое описание: Повышение привилегий в Windows Accessibility Infrastructure

Идентификатор уязвимости: CVE-2026-24291
BDU:2026-03020

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: Microsoft Corp Windows Server 2012 R2 (Server Core installation) до 6.3.9600.23074
Microsoft Corp Windows Server 2012 R2 до 6.3.9600.23074
Microsoft Corp Windows Server 2012 (Server Core installation) до 6.2.9200.25973
Microsoft Corp Windows Server 2012 до 6.2.9200.25973
Microsoft Corp Windows 10 1607 до 10.0.14393.8957 64-bit

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-13 / 2026-03-20

Ссылки на источник:

- https://bdu.fstec.ru/vul/2026-03020
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24291
- https://github.com/mdsecactivebreach/RegPwn