НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-06-25.1 | 25 июня 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-47952	Adobe Reader	Локальный	ACE	2026-06-11	✔
2	Критическая	CVE-2026-41293	Apache Tomcat	Сетевой	DoS	2026-06-09	✔
3	Высокая	CVE-2026-41284	Apache Tomcat	Сетевой	DoS	2026-06-09	✔
4	Критическая	CVE-2026-43512	Apache Tomcat	Сетевой	PE	2026-06-09	✔
5	Критическая	CVE-2026-43515	Apache Tomcat	Сетевой	OSI	2026-06-09	✔
6	Высокая	CVE-2026-43514	Apache Tomcat	Сетевой	OSI	2026-06-09	✔
7	Высокая	CVE-2026-48563	Windows	Сетевой	ACE	2026-06-10	✔
8	Высокая	CVE-2026-47912	Adobe Reader	Локальный	ACE	2026-06-11	✔
9	Высокая	CVE-2026-47913	Adobe Reader	Локальный	ACE	2026-06-11	✔
10	Высокая	CVE-2026-32193	Azure Kubernetes Service	Локальный	ACE	2026-06-10	✔
11	Высокая	CVE-2026-42987	Windows Server	Сетевой	ACE	2026-06-10	✔
12	Высокая	CVE-2026-44810	Windows	Локальный	PE	2026-06-10	✔
13	Критическая	CVE-2026-44815	Windows	Сетевой	ACE	2026-06-11	✔

14	Высокая	CVE-2026-45641	Windows	Локальный	ACE	2026-06-10	✔
15	Высокая	CVE-2026-42992	Windows	Сетевой	ACE	2026-06-10	✔
16	Высокая	CVE-2026-45648	Windows Server	Сетевой	ACE	2026-06-10	✔
17	Высокая	CVE-2026-44799	Windows	Сетевой	ACE	2026-06-11	✔
18	Высокая	CVE-2026-42993	Windows	Сетевой	ACE	2026-06-10	✔
19	Высокая	CVE-2026-42986	Windows	Локальный	PE	2026-06-10	✔
20	Высокая	CVE-2026-11235	Google Chrome и Microsoft Edge	Сетевой	ACE	2026-06-08	✔
21	Высокая	CVE-2026-45472	Microsoft Office	Локальный	ACE	2026-06-10	✔
22	Высокая	CVE-2026-42909	Windows	Сетевой	ACE	2026-06-10	✔
23	Высокая	CVE-2026-45644	Microsoft Live Share Canvas SDK	Сетевой	PE	2026-06-15	✔
24	Высокая	CVE-2026-42905	Windows	Локальный	PE	2026-06-10	✔
25	Критическая	CVE-2026-42904	Windows	Смежная сеть	PE	2026-06-10	✔
26	Высокая	CVE-2026-45474	Microsoft Office	Локальный	ACE	2026-06-11	✔
27	Высокая	CVE-2026-42979	Windows	Локальный	PE	2026-06-10	✔
28	Высокая	CVE-2026-42981	Windows	Сетевой	ACE	2026-06-10	✔

29	Высокая	CVE-2026-42974	Windows	Сетевой	ACE	2026-06-10	✔
30	Высокая	CVE-2026-42991	Windows	Локальный	PE	2026-06-10	✔
31	Высокая	CVE-2026-45461	Microsoft Office	Локальный	ACE	2026-06-10	✔
32	Высокая	CVE-2026-44812	Windows	Локальный	ACE	2026-06-11	✔
33	Высокая	CVE-2026-45607	Windows	Локальный	ACE	2026-06-11	✔
34	Высокая	CVE-2026-45456	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-10	✔
35	Высокая	CVE-2026-45471	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-15	✔
36	Критическая	CVE-2026-47643	Azure Stack Edge	Сетевой	ACE	2026-06-15	✔
37	Критическая	CVE-2026-45602	Windows	Сетевой	OSI	2026-06-15	✔
38	Высокая	CVE-2026-44803	Windows Graphics Componen	Локальный	ACE	2026-06-11	✔
39	Высокая	CVE-2026-45484	Microsoft SharePoint Server Subscription Edition	Сетевой	PE	2026-06-15	✔
40	Высокая	BDU:2026-08226	RuBackup	Сетевой	DoS	2026-06-08	✔
41	Высокая	BDU:2026-08231	RuBackup	Смежная сеть	PE	2026-06-08	✔
42	Высокая	CVE-2026-48568	Windows	Локальный	SB	2026-06-15	✔

43	Высокая	CVE-2026-45643	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-15	✔
44	Высокая	CVE-2026-48565	Narrator	Локальный	PE	2026-06-15	✔
45	Высокая	CVE-2026-47631	Microsoft Exchange Server Subscription Edition RTM	Сетевой	SB	2026-06-15	✔
46	Высокая	CVE-2026-45605	Windows	Локальный	PE	2026-06-15	✔
47	Высокая	CVE-2026-44807	Windows	Локальный	PE	2026-06-15	✔
48	Высокая	CVE-2026-42977	Windows	Локальный	PE	2026-06-15	✔
49	Высокая	CVE-2026-42908	Windows	Сетевой	OSI	2026-06-15	✔
50	Высокая	CVE-2026-33828	Windows	Локальный	PE	2026-06-10	✔
51	Высокая	CVE-2026-11236	Google Chrome	Сетевой	Не определено	2026-06-08	✔
52	Высокая	CVE-2026-48293	Adobe InDesign	Локальный	ACE	2026-06-10	✔
53	Высокая	CVE-2026-11224	Google Chrome	Сетевой	ACE	2026-06-08	✔
54	Высокая	CVE-2026-52884	Notepad++	Локальный	ACE	2026-06-15	✔
55	Высокая	CVE-2026-44813	Windows	Локальный	PE	2026-06-15	✔
56	Высокая	CVE-2016-6581	hpack	Сетевой	DoS	2026-06-09	✔

57	Высокая	CVE-2026-24187	vGPU	Локальный	ACE	2026-06-09	✔
58	Критическая	CVE-2026-26980	Ghost	Сетевой	OSI	2026-06-09	✔
59	Высокая	CVE-2026-44804	Windows	Локальный	PE	2026-06-15	✔
60	Высокая	CVE-2026-50257	Red Hat Enterprise Linux	Локальный	DoS	2026-06-09	✔
61	Высокая	CVE-2026-50258	Red Hat Enterprise Linux	Локальный	DoS	2026-06-09	✔
62	Высокая	CVE-2026-50259	Red Hat Enterprise Linux	Локальный	DoS	2026-06-09	✔
63	Высокая	CVE-2026-50260	Red Hat Enterprise Linux	Локальный	DoS	2026-06-09	✔
64	Высокая	CVE-2026-50261	Red Hat Enterprise Linux	Локальный	DoS	2026-06-09	✔
65	Критическая	CVE-2026-8153	PolyScope	Сетевой	ACE	2026-06-09	✔
66	Высокая	CVE-2026-8945	Firefox	Сетевой	ACE	2026-06-09	✔
67	Высокая	CVE-2026-8946	Firefox	Сетевой	ACE	2026-06-09	✔
68	Высокая	CVE-2026-11237	Google Chrome	Сетевой	SUI	2026-06-08	✔
69	Критическая	CVE-2026-8948	Firefox	Сетевой	ACE	2026-06-09	✔
70	Критическая	CVE-2026-34084	PhpSpreadsheet	Сетевой	ACE	2026-06-15	✔
71	Высокая	CVE-2026-42913	Windows	Сетевой	ACE	2026-06-15	✔

72	Высокая	CVE-2026-44819	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-15	✔️
73	Высокая	CVE-2026-48575	Windows	Локальный	SB	2026-06-15	✔️
74	Высокая	CVE-2026-45645	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-15	✔️
75	Высокая	CVE-2026-48583	Windows	Локальный	PE	2026-06-15	✔️
76	Высокая	CVE-2026-42989	Windows	Локальный	PE	2026-06-15	✔️
77	Высокая	CVE-2026-44809	Windows	Локальный	PE	2026-06-15	✔️
78	Высокая	CVE-2026-44811	Windows	Локальный	PE	2026-06-15	✔️
79	Высокая	CVE-2026-42983	Windows	Локальный	PE	2026-06-15	✔️
80	Высокая	CVE-2026-44802	Windows	Локальный	PE	2026-06-15	✔️
81	Высокая	CVE-2026-47656	Windows	Локальный	SB	2026-06-15	✔️
82	Высокая	CVE-2026-11231	Google Chrome	Сетевой	ACE	2026-06-08	✔️
83	Высокая	CVE-2026-11230	Google Chrome	Сетевой	ACE	2026-06-08	✔️
84	Высокая	CVE-2026-44808	Windows	Локальный	PE	2026-06-15	✔️
85	Высокая	CVE-2026-42978	Windows	Локальный	PE	2026-06-15	✔️

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47952
BDU:2026-08091

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

Уязвимый продукт: Adobe Reader: до 26.001.21662
Adobe Acrobat: до 26.001.21662
Adobe Acrobat 2024: до 24.001.30383

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08091

2

Краткое описание: Отказ в обслуживании в Apache Tomcat

Идентификатор уязвимости: CVE-2026-41293
BDU:2026-08085

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Tomcat: от 9.0.0.M1 до 9.0.117 включительно
Ubuntu: 26.04 LTS
Jboss Web Server: 6
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-r29c-68gh-xp6x
- https://github.com/apache/tomcat/commit/f72a6174ab1f0f5a053435f80448b4f6837fe6d7
- https://github.com/apache/tomcat/commit/19f17a257797e8d139b33ff9c88d362a273be148
- https://tomcat.apache.org/security-10.html
- https://github.com/apache/tomcat
- https://github.com/apache/tomcat/commit/1c70480466572c9192ed412ebefcd43fc63137fd
- https://github.com/apache/tomcat/commit/cf9452443bcbf3b1a4b435ef7d624364f1b65ca3

- https://github.com/apache/tomcat/commit/3915fd27e6810b14ccd21e3d900bd8faef44d3df
- https://github.com/apache/tomcat/commit/e5cef9618c3f4fd31bd6fb1e83f0f18022280dac
- https://github.com/apache/tomcat/commit/2a2476460e823789f530a22207873ea8cd6eff3b
- https://access.redhat.com/security/cve/cve-2026-41293
- https://ubuntu.com/security/CVE-2026-41293
- https://security-tracker.debian.org/tracker/CVE-2026-41293
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-41293
- https://bdu.fstec.ru/vul/2026-08085

3

Краткое описание: Отказ в обслуживании в Apache Tomcat

Идентификатор уязвимости: CVE-2026-41284
BDU:2026-08084

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

Уязвимый продукт: Tomcat: от 9.0.0.M1 до 9.0.117 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-gx5v-xp9w-j4cg
- https://tomcat.apache.org/security-10.html
- https://github.com/apache/tomcat
- https://github.com/apache/tomcat/commit/17dacd9aa48628da2eba37a9ab743c0b6c71685c
- https://github.com/apache/tomcat/commit/a96fffd18487a29c0a30d36f00cb2b2d91f6d42c
- https://tomcat.apache.org/security-11.html
- https://github.com/apache/tomcat/commit/b3d1c1c239142e806be0b7329d304b94a58913ed
- http://www.openwall.com/lists/oss-security/2026/05/12/12
- https://tomcat.apache.org/security-9.html
- https://lists.apache.org/thread/2nvqjr7ovjmvx2vbhb7s61ycd5msc8qc
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-41284
- https://security-tracker.debian.org/tracker/CVE-2026-41284
- https://ubuntu.com/security/CVE-2026-41284
- https://bdu.fstec.ru/vul/2026-08084

4

Краткое описание: Повышение привилегий в Apache Tomcat

Идентификатор уязвимости: CVE-2026-43512
BDU:2026-08081

Идентификатор программной ошибки: CWE-592 НЕ РЕКОМЕНДУЕТСЯ: Уязвимости, связанные с обходом аутентификации

Уязвимый продукт: Tomcat: от 10.1.0-M1 до 10.1.54 включительно
Ubuntu: 26.04 LTS
Jboss Web Server: 6
Debian GNU/Linux: 13
РЕД ОС: 8.0
Red Hat Process Automation: 7
OpenShift Dev Spaces: -
Red Hat Hardened Images: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Повышение привилегий

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

только после оценки всех сопутствующих рисков.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-h6fc-48rj-7qqh
- https://github.com/apache/tomcat/commit/6565a6cb6499e56fe2f34457cec99f9d1c4f39e9
- https://lists.apache.org/thread/7x09x7o12solvclslw3sz0288xc8wx73
- http://www.openwall.com/lists/oss-security/2026/05/12/8
- https://tomcat.apache.org/security-10.html
- https://github.com/apache/tomcat/commit/a99c355e8199adbfd67c9a1fffbd85b810b196cd
- https://tomcat.apache.org/security-11.html
- https://github.com/apache/tomcat/commit/3d4d3fae07a6cd9c2eb193c5491001740ec64448
- https://tomcat.apache.org/security-9.html
- https://ubuntu.com/security/CVE-2026-43512
- https://security-tracker.debian.org/tracker/CVE-2026-43512
- https://access.redhat.com/security/cve/cve-2026-43512
- https://github.com/covepseng/cve-2026-43512-poc
- https://bdu.fstec.ru/vul/2026-08081

5

Краткое описание: Получение конфиденциальной информации в Apache Tomcat

Идентификатор уязвимости: CVE-2026-43515
BDU:2026-08080

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Tomcat: от 10.1.0-M1 до 10.1.54 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-5m62-pw8w-7w9f
- https://github.com/apache/tomcat/commit/db919ff9912b4d61d1b702a1342b8bde39270031
- https://tomcat.apache.org/security-10.html
- https://lists.apache.org/thread/746nxfxod0wsocxtmv8pb8nkgmwpc6bb
- https://github.com/apache/tomcat
- http://www.openwall.com/lists/oss-security/2026/05/12/11
- https://github.com/apache/tomcat/commit/c621317382682206fb58ab92ebd3e1b6fdd10ce9
- https://tomcat.apache.org/security-11.html
- https://tomcat.apache.org/security-9.html
- https://github.com/apache/tomcat/commit/276087d9c7abbcecc6c4fb4e4b08cf64780c6e36
- https://security-tracker.debian.org/tracker/CVE-2026-43515
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-43515
- https://ubuntu.com/security/CVE-2026-43515
- https://bdu.fstec.ru/vul/2026-08080

6

Краткое описание: Получение конфиденциальной информации в Apache Tomcat

Идентификатор уязвимости: CVE-2026-43514
BDU:2026-08079

Идентификатор программной ошибки: CWE-208 Разглашение информации, связанное с временной разницей при выполнении операций

Уязвимый продукт: Tomcat: от 10.1.0-M1 до 10.1.54 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-9m89-8frq-c98c
- https://tomcat.apache.org/security-10.html
- https://lists.apache.org/thread/2k654v5cq123npfsd1b2kk1y30owqb1m
- https://github.com/apache/tomcat
- https://github.com/apache/tomcat/commit/933dcdbf2515972280002929e7e597dead2e9ffa
- https://tomcat.apache.org/security-11.html
- http://www.openwall.com/lists/oss-security/2026/05/12/10
- https://tomcat.apache.org/security-9.html
- https://github.com/apache/tomcat/commit/d35d9d23263c8e4af561f615c960c91697ff200e
- https://github.com/apache/tomcat/commit/a102a2a157868ca51d83eaf5a119ccd9976a113e
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-43514

- https://ubuntu.com/security/CVE-2026-43514
- https://security-tracker.debian.org/tracker/CVE-2026-43514
- https://bdu.fstec.ru/vul/2026-08079

7

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-48563
BDU:2026-08119

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48563
- https://bdu.fstec.ru/vul/2026-08119

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47912
BDU:2026-08104

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader: до 26.001.21662
Adobe Acrobat: до 26.001.21662
Adobe Acrobat 2024: до 24.001.30383

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08104

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47913
BDU:2026-08089

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader: до 26.001.21662
Adobe Acrobat: до 26.001.21662
Adobe Acrobat 2024: до 24.001.30383

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08089

10

Краткое описание: Выполнение произвольного кода в Azure Kubernetes Service

Идентификатор уязвимости: CVE-2026-32193
BDU:2026-08120

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

Уязвимый продукт: Azure Kubernetes Service: до v0.20260213.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV: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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32193
- https://bdu.fstec.ru/vul/2026-08120

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2026-42987
BDU:2026-08127

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

1
1

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42987
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08127

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44810
BDU:2026-08128

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

1
2

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: 8.4 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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44810

- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08128

13

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-44815
BDU:2026-08129

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44815
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08129

14

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-45641
BDU:2026-08130

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

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45641
- https://bdu.fstec.ru/vul/2026-08130

15

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42992
BDU:2026-08131

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655

Windows 11 26H1: до 10.0.28000.2269
Windows App Client for Windows Desktop: до 2.0.1193.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42992
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08131

16

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2026-45648
BDU:2026-08132

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45648
- https://bdu.fstec.ru/vul/2026-08132

17

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-44799
BDU:2026-08133

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228

Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Remote Desktop client for Windows Desktop: до 1.2.7214.0
Windows App Client for Windows Desktop: до 2.0.1193.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44799
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08133

18

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42993
BDU:2026-08134

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

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42993
- https://bdu.fstec.ru/vul/2026-08134

19

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42986
BDU:2026-08135

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42986
- https://bdu.fstec.ru/vul/2026-08135

20

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2026-11235
BDU:2026-08126

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

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: 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.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11235
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11235
- https://security-tracker.debian.org/tracker/CVE-2026-11235
- https://bdu.fstec.ru/vul/2026-08126

21

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-45472
BDU:2026-08217

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: -
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2016: до 16.0.5556.1005
Microsoft Office 2019: -
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45472
- https://bdu.fstec.ru/vul/2026-08217

22

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42909
BDU:2026-08216

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42909
- https://bdu.fstec.ru/vul/2026-08216

Краткое описание: Повышение привилегий в Microsoft Live Share Canvas SDK

Идентификатор уязвимости: CVE-2026-45644
BDU:2026-08215

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

Уязвимый продукт: Microsoft Live Share Canvas SDK: до 1.4.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Повышение привилегий

2 3 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45644
- https://bdu.fstec.ru/vul/2026-08215

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42905
BDU:2026-08214

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Windows 11 26H1 - extra: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42905
- https://bdu.fstec.ru/vul/2026-08214

25

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42904
BDU:2026-08213

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Windows 11 26H1 - extra: до 10.0.28000.2269

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42904
- https://bdu.fstec.ru/vul/2026-08213

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-45474
BDU:2026-08212

Идентификатор программной ошибки: CWE-416 Использование после освобождения

26 **Уязвимый продукт:** Microsoft Office: -
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2016: до 16.0.5556.1005
Microsoft Office 2019: -
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45474
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08212

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42979
BDU:2026-08202

Идентификатор программной ошибки: CWE-416 Использование после освобождения

27

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256

Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42979
- https://bdu.fstec.ru/vul/2026-08202

28

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42981
BDU:2026-08206

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995

Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42981
- https://bdu.fstec.ru/vul/2026-08206

29

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42974
BDU:2026-08205

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

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42974
- https://bdu.fstec.ru/vul/2026-08205

30

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42991
BDU:2026-08204

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880

Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42991
- https://bdu.fstec.ru/vul/2026-08204

31

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-45461
BDU:2026-08218

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Microsoft Office 2016: до 16.0.5556.1005
Microsoft Office 2019: -
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45461
- https://bdu.fstec.ru/vul/2026-08218

32

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-44812
BDU:2026-08200

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

Уязвимый продукт: Microsoft Word: -
Microsoft Excel: -
Microsoft PowerPoint: -
Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880

Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44812
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08200

33

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-45607
BDU:2026-08210

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45607
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08210

34

Краткое описание: Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-45456
BDU:2026-08219

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20384
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5556.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5556.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20153
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45456
- https://bdu.fstec.ru/vul/2026-08219

35

Краткое описание: Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-45471
BDU:2026-08223

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20384
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5556.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5556.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20153
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45471
- https://bdu.fstec.ru/vul/2026-08223

36

Краткое описание: Выполнение произвольного кода в Azure Stack Edge

Идентификатор уязвимости: CVE-2026-47643
BDU:2026-08221

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: Azure Stack Edge: до 3.3.2604.3097

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47643
- https://bdu.fstec.ru/vul/2026-08221

37

Краткое описание: Получение конфиденциальной информации в Windows

Идентификатор уязвимости: CVE-2026-45602
BDU:2026-08222

Идентификатор программной ошибки: CWE-229 Некорректная обработка значений

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602
- https://bdu.fstec.ru/vul/2026-08222

38

Краткое описание: Выполнение произвольного кода в Windows Graphics Componen

Идентификатор уязвимости: CVE-2026-44803
BDU:2026-08199

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

Уязвимый продукт: Microsoft Word: -
Microsoft Excel: -
Microsoft PowerPoint: -
Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256

Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-11 / 2026-06-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44803
- https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-security-update-review
- https://bdu.fstec.ru/vul/2026-08199

39

Краткое описание: Повышение привилегий в Microsoft SharePoint Server Subscription Edition

Идентификатор уязвимости: CVE-2026-45484
BDU:2026-08225

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: 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45484
- https://bdu.fstec.ru/vul/2026-08225

40

Краткое описание: Отказ в обслуживании в RuBackup

Идентификатор уязвимости: BDU:2026-08226

Идентификатор программной ошибки: CWE-410 Недостаточный пул ресурсов

Уязвимый продукт: RuBackup: до 2.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://www.rubackup.ru/
- https://lk.astra.ru/
- https://wiki.astralinux.ru/x/ziLoD
- https://bdu.fstec.ru/vul/2026-08226

41

Краткое описание: Повышение привилегий в RuBackup

Идентификатор уязвимости: BDU:2026-08231

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: RuBackup: до 2.7

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.rubackup.ru/
- https://lk.astra.ru/
- https://wiki.astralinux.ru/x/ziLoD
- https://bdu.fstec.ru/vul/2026-08231

42

Краткое описание: Обход безопасности в Windows

Идентификатор уязвимости: CVE-2026-48568
BDU:2026-08234

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655

Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48568
- https://bdu.fstec.ru/vul/2026-08234

4 **Краткое описание:** Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

3	**Идентификатор уязвимости:** CVE-2026-45643 BDU:2026-08235 **Идентификатор программной ошибки:** CWE-822 Разыменование непроверенного указателя **Уязвимый продукт:** Microsoft 365 Apps for Enterprise: - Microsoft Office LTSC 2021: - Microsoft Office LTSC 2024: - Microsoft Office 365: - **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Манипулирование структурами данных. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Оценка CVSSv4:** Не определено **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2026-06-15 / 2026-06-15 **Ссылки на источник:** • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45643 • https://bdu.fstec.ru/vul/2026-08235
4	**Краткое описание:** Повышение привилегий в Narrator
4	**Идентификатор уязвимости:** CVE-2026-48565

BDU:2026-08237

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Narrator: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48565
- https://bdu.fstec.ru/vul/2026-08237

45

Краткое описание: Обход безопасности в Microsoft Exchange Server Subscription Edition RTM

Идентификатор уязвимости: CVE-2026-47631

BDU:2026-08239

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

Уязвимый продукт: Microsoft Exchange Server Subscription Edition RTM: до 15.02.2562.043
Microsoft Exchange Server 2019 Cumulative Update 15: до 15.02.1748.046
Microsoft Exchange Server 2019 Cumulative Update 14: до 15.02.1544.041
Microsoft Exchange Server 2016 Cumulative Update 23: до 15.01.2507.069

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 8.1 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47631
- https://bdu.fstec.ru/vul/2026-08239

4
6

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-45605
BDU:2026-08240

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт:
Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45605
- https://bdu.fstec.ru/vul/2026-08240

47

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44807
BDU:2026-08241

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44807
- https://bdu.fstec.ru/vul/2026-08241

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42977
BDU:2026-08242

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

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

4
8

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42977
- https://bdu.fstec.ru/vul/2026-08242

49

Краткое описание: Получение конфиденциальной информации в Windows

Идентификатор уязвимости: CVE-2026-42908
BDU:2026-08248

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Windows App Client for Windows Desktop: до 2.0.1193.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42908
- https://bdu.fstec.ru/vul/2026-08248

50

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-33828
BDU:2026-08220

Идентификатор программной ошибки: CWE-501 Нарушение границ доверия

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33828
- https://bdu.fstec.ru/vul/2026-08220

51

Краткое описание: Уязвимость в Google Chrome

Идентификатор уязвимости: CVE-2026-11236
BDU:2026-08195

Идентификатор программной ошибки: CWE-602 Обеспечение безопасности сервера на стороне клиента

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Не определено

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

Оценка CVSSv3: 8.3 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.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11236
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11236
- https://security-tracker.debian.org/tracker/CVE-2026-11236
- https://bdu.fstec.ru/vul/2026-08195

52

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-48293
BDU:2026-08184

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08184

53

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11224
BDU:2026-08193

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

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: 8.1 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11224
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11224
- https://security-tracker.debian.org/tracker/CVE-2026-11224
- https://bdu.fstec.ru/vul/2026-08193

Краткое описание: Выполнение произвольного кода в Notepad++

Идентификатор уязвимости: CVE-2026-52884
BDU:2026-08136

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

Уязвимый продукт: Notepad++: 8.9.6.1

5
4

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: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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://news.ycombinator.com/item?id=48473731
- https://github.com/notepad-plus-plus/notepad-plus-plus/security/advisories/GHSA-p58x-r3c9-x9p6
- https://bdu.fstec.ru/vul/2026-08136

55

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44813
BDU:2026-08137

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44813
- https://bdu.fstec.ru/vul/2026-08137

Краткое описание: Отказ в обслуживании в hpack

Идентификатор уязвимости: CVE-2016-6581
BDU:2026-08138

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

Уязвимый продукт: hpack: от 1.0.0 до 2.2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://python-hyper.org/hpack/en/latest/security/CVE-2016-6581.html
- http://www.securityfocus.com/bid/92315
- https://bdu.fstec.ru/vul/2026-08138

Краткое описание: Выполнение произвольного кода в vGPU

Идентификатор уязвимости: CVE-2026-24187
BDU:2026-08139

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: vGPU: до 16.14
Cloud Gaming Guest Driver: до 535.309.01
Cloud Gaming Virtual GPU Manager: до 595.71.03
NVS R535: до 539.72
Tesla R535: до 539.72
NVIDIA RTX R535: до 539.72
Quadro R535: до 539.72
GeForce R580: до 582.53
NVIDIA RTX R580: до 582.53
Tesla R580: до 582.53
GeForce R595: до 596.36
NVIDIA RTX R595: до 596.36
Tesla R595: до 596.36
NVS R595: до 596.36
Quadro R595: до 596.36
NVS R580: до 582.53
Quadro R580: до 582.53

Категория уязвимого продукта: Не определено

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://nvidia.custhelp.com/app/answers/detail/a_id/5821/~/security-bulletin%3A-nvidia-gpu-display-drivers---may-2026
- https://bdu.fstec.ru/vul/2026-08139

Краткое описание: Получение конфиденциальной информации в Ghost

Идентификатор уязвимости: CVE-2026-26980
BDU:2026-08140

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

Уязвимый продукт: Ghost: до 6.19.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

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.

58

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/TryGhost/Ghost/security/advisories/GHSA-w52v-v783-gw97
- https://github.com/TryGhost/Ghost/commit/30868d632b2252b638bc8a4c8ebf73964592ed91
- https://github.com/TryGhost/Ghost/releases/tag/v6.19.1
- https://blog.xlab.qianxin.com/ghost-cms-mass-compromised-via-cve-2026-26980-now-fueling-clickfix-attacks/

- https://bdu.fstec.ru/vul/2026-08140

59

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44804
BDU:2026-08142

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44804
- https://bdu.fstec.ru/vul/2026-08142

60

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-50257
BDU:2026-08143

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Red Hat Enterprise Linux: 10
X.Org Server: до 21.1.23
XWayland: до 24.1.12

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-50257
- https://bugzilla.redhat.com/show_bug.cgi?id=2485382
- https://gitlab.freedesktop.org/xorg/xserver/-/commit/f5abfb61994471023d8c6470428c8e30c411cc0b
- https://lists.x.org/archives/xorg-announce/2026-June/003702.html
- https://redhat.atlassian.net/browse/PSIRTSUPT-16950
- https://bdu.fstec.ru/vul/2026-08143

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-50258
BDU:2026-08144

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Red Hat Enterprise Linux: 10
X.Org Server: до 21.1.23
XWayland: до 24.1.12

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.

6
1

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-50258
- https://bugzilla.redhat.com/show_bug.cgi?id=2485383
- https://gitlab.freedesktop.org/xorg/xserver/-/commit/543e108516428fc8c3bea91d6563ad266f9a801e
- https://lists.x.org/archives/xorg-announce/2026-June/003702.html
- https://redhat.atlassian.net/browse/PSIRTSUPT-16950
- https://bdu.fstec.ru/vul/2026-08144

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-50259
BDU:2026-08145

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Red Hat Enterprise Linux: 10
X.Org Server: до 21.1.23
XWayland: до 24.1.12

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.

6
2

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-50259
- https://bugzilla.redhat.com/show_bug.cgi?id=2485384
- https://gitlab.freedesktop.org/xorg/xserver/-/commit/867b59b33bee669cb412f1314e47c52eacf6e00b
- https://lists.x.org/archives/xorg-announce/2026-June/003702.html
- https://redhat.atlassian.net/browse/PSIRTSUPT-16950
- https://bdu.fstec.ru/vul/2026-08145

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-50260
BDU:2026-08146

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Red Hat Enterprise Linux: 10
X.Org Server: до 21.1.23
XWayland: до 24.1.12

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.

6
3

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-50260
- https://bugzilla.redhat.com/show_bug.cgi?id=2485385
- https://gitlab.freedesktop.org/xorg/xserver/-/commit/f5abfb61994471023d8c6470428c8e30c411cc0b
- https://lists.x.org/archives/xorg-announce/2026-June/003702.html
- https://redhat.atlassian.net/browse/PSIRTSUPT-16950
- https://bdu.fstec.ru/vul/2026-08146

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-50261
BDU:2026-08147

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Red Hat Enterprise Linux: 10
X.Org Server: до 21.1.23
XWayland: до 24.1.12

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.

64

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://access.redhat.com/security/cve/CVE-2026-50261
- https://bugzilla.redhat.com/show_bug.cgi?id=2485386
- https://gitlab.freedesktop.org/xorg/xserver/-/commit/bdd7bf57af208b1ddf57d4683d67104443b44812
- https://lists.x.org/archives/xorg-announce/2026-June/003702.html
- https://redhat.atlassian.net/browse/PSIRTSUPT-16950
- https://bdu.fstec.ru/vul/2026-08147

Краткое описание: Выполнение произвольного кода в PolyScope

Идентификатор уязвимости: CVE-2026-8153
BDU:2026-08153

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

Уязвимый продукт: PolyScope: до 5.25.1

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

6 5 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://www.universal-robots.com/developer/communication-protocol/dashboard-server/
- https://bdu.fstec.ru/vul/2026-08153

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8945
BDU:2026-08154

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Firefox: до 151

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://bdu.fstec.ru/vul/2026-08154

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8946
BDU:2026-08155

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

Уязвимый продукт: Firefox: до 151
Firefox ESR: до 140.11
Thunderbird: до 140.11

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.

6
7

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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-47/
- https://www.mozilla.org/security/advisories/mfsa2026-48/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://www.mozilla.org/security/advisories/mfsa2026-51/
- https://bdu.fstec.ru/vul/2026-08155

Краткое описание: Пользовательский интерфейс подмены в Google Chrome

Идентификатор уязвимости: CVE-2026-11237
BDU:2026-08194

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Пользовательский интерфейс подмены

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

68

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.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11237
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11237
- https://security-tracker.debian.org/tracker/CVE-2026-11237
- https://bdu.fstec.ru/vul/2026-08194

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-8948
BDU:2026-08157

Идентификатор программной ошибки: CWE-1004 Отсутствие флага HttpOnly у конфиденциальных куки-параметров

Уязвимый продукт: Firefox: до 151
Thunderbird: до 151

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Выполнение произвольного кода

69 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-46/
- https://www.mozilla.org/security/advisories/mfsa2026-50/
- https://bdu.fstec.ru/vul/2026-08157

Краткое описание: Выполнение произвольного кода в PhpSpreadsheet

Идентификатор уязвимости: CVE-2026-34084
BDU:2026-08159

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

Уязвимый продукт: PhpSpreadsheet: до 1.30.2 включительно

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.

70

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://github.com/PHPOffice/PhpSpreadsheet/security/advisories/GHSA-q4q6-r8wh-5cgh
- https://dailycve.com/phpspreadsheet-phar-wrapper-bypass-cve-2026-34084-critical-dc-jun2026-303/
- https://bdu.fstec.ru/vul/2026-08159

7
1

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42913
BDU:2026-08164

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Remote Desktop client for Windows Desktop: до 1.2.7214.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42913
- https://bdu.fstec.ru/vul/2026-08164

Краткое описание: Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-44819
BDU:2026-08168

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20384
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2016: до 16.0.5556.1005
Microsoft Office 2019: -
Microsoft SharePoint Enterprise Server 2016: до 16.0.5556.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20153
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

7
2

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44819
- https://bdu.fstec.ru/vul/2026-08168

7
3

Краткое описание: Обход безопасности в Windows

Идентификатор уязвимости: CVE-2026-48575
BDU:2026-08169

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48575
- https://bdu.fstec.ru/vul/2026-08169

7
4

Краткое описание: Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-45645
BDU:2026-08170

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2016: до 16.0.5556.1001
Microsoft Office 2019: -
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45645
- https://bdu.fstec.ru/vul/2026-08170

75

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-48583
BDU:2026-08171

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48583
- https://bdu.fstec.ru/vul/2026-08171

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42989
BDU:2026-08172

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880

Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42989
- https://bdu.fstec.ru/vul/2026-08172

77

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44809
BDU:2026-08173

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8655
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995

Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44809
- https://bdu.fstec.ru/vul/2026-08173

78

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44811
BDU:2026-08174

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44811
- https://bdu.fstec.ru/vul/2026-08174

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42983
BDU:2026-08175

7
9

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655

Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42983
- https://bdu.fstec.ru/vul/2026-08175

80

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44802
BDU:2026-08176

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417

Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44802
- https://bdu.fstec.ru/vul/2026-08176

81

Краткое описание: Обход безопасности в Windows

Идентификатор уязвимости: CVE-2026-47656
BDU:2026-08180

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт:
Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47656
- https://bdu.fstec.ru/vul/2026-08180

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11231
BDU:2026-08186

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

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

8
2

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-08 / 2026-06-08

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11231

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11231
- https://security-tracker.debian.org/tracker/CVE-2026-11231
- https://bdu.fstec.ru/vul/2026-08186

83

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11230
BDU:2026-08190

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52
Debian GNU/Linux: 13
Fedora EPEL: epel10

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.html
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2026-11230
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-11230

- https://security-tracker.debian.org/tracker/CVE-2026-11230
- https://bdu.fstec.ru/vul/2026-08190

84

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-44808
BDU:2026-08158

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44808
- https://bdu.fstec.ru/vul/2026-08158

8
5

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-42978
BDU:2026-08249

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

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: 2026-06-15 / 2026-06-15

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42978
- https://bdu.fstec.ru/vul/2026-08249