НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-05-26.1 | 26 мая 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-29609	OpenClaw	Сетевой	DoS	2026-04-30	✓
2	Высокая	BDU:2026-06201	PostgreSQL	Локальный	DoS	2026-05-04	✓
3	Высокая	BDU:2026-06214	Astra Linux Special Edition	Сетевой	DoS	2026-05-04	✓
4	Высокая	BDU:2026-06228	libvirt	Сетевой	DoS	2026-05-04	✓
5	Высокая	BDU:2026-06252	CUPS	Сетевой	DoS	2026-05-04	✓
6	Высокая	BDU:2026-06276	astra-safepolicy	Локальный	DoS	2026-05-04	✓
7	Критическая	CVE-2026-41940	cPanel	Сетевой	ACE	2026-05-04	✓
8	Высокая	CVE-2026-5979	DIR-605L	Сетевой	ACE	2026-05-04	✓
9	Высокая	CVE-2026-7470	Tenda 4G300	Сетевой	DoS	2026-05-04	✓
10	Высокая	CVE-2026-6015	Tenda AC9	Сетевой	DoS	2026-05-04	✓
11	Высокая	CVE-2026-6016	Tenda AC9	Сетевой	DoS	2026-05-04	✓
12	Высокая	BDU:2026-06173	Suricata	Сетевой	DoS	2026-04-30	✓
13	Высокая	CVE-2026-31935	Suricata	Сетевой	DoS	2026-04-30	✓

14	Высокая	CVE-2026-31934	Suricata	Сетевой	DoS	2026-04-30	✓
15	Высокая	CVE-2026-31933	Suricata	Сетевой	DoS	2026-04-30	✓
16	Высокая	CVE-2026-31937	Suricata	Сетевой	DoS	2026-04-30	✓
17	Высокая	CVE-2026-31932	Suricata	Сетевой	DoS	2026-04-30	✓
18	Высокая	CVE-2026-7750	TOTOLINK N300RH	Сетевой	DoS	2026-05-05	✓
19	Высокая	CVE-2026-7748	TOTOLINK N300RH	Сетевой	ACE	2026-05-05	✓
20	Высокая	CVE-2026-2885	D-Link DWR-M960	Сетевой	ACE	2026-05-04	✓
21	Высокая	CVE-2026-2857	D-Link DWR-M960	Сетевой	ACE	2026-05-04	✓
22	Высокая	CVE-2026-2856	D-Link DWR-M960	Сетевой	ACE	2026-05-04	✓
23	Высокая	CVE-2026-2853	D-Link DWR-M960	Сетевой	ACE	2026-05-04	✓
24	Высокая	CVE-2026-7855	DI-8100	Сетевой	DoS	2026-05-06	✓
25	Критическая	CVE-2026-7853	DI-8100	Сетевой	ACE	2026-05-06	✓
26	Критическая	CVE-2026-7854	DI-8100	Сетевой	DoS	2026-05-06	✓
27	Критическая	CVE-2026-42375	DIR-600L	Сетевой	PE	2026-05-06	✓
28	Критическая	CVE-2026-42376	DIR-456U	Сетевой	PE	2026-05-06	✓

29	Высокая	CVE-2026-42372	DIR-605L	Смежная сеть	PE	2026-05-06	✓
30	Критическая	CVE-2026-42373	DIR-605L	Сетевой	PE	2026-05-06	✓
31	Критическая	CVE-2026-42374	DIR-600L	Сетевой	PE	2026-05-06	✓
32	Высокая	CVE-2026-7032	Tenda F456	Сетевой	DoS	2026-05-06	✓
33	Высокая	CVE-2026-7102	Tenda F456	Сетевой	ACE	2026-05-06	✓
34	Высокая	CVE-2026-7078	Tenda F456	Сетевой	DoS	2026-05-06	✓
35	Высокая	CVE-2026-7019	Tenda F456	Сетевой	ACE	2026-05-06	✓
36	Высокая	CVE-2026-7033	Tenda F456	Сетевой	ACE	2026-05-06	✓
37	Высокая	CVE-2026-7031	Tenda F456	Сетевой	DoS	2026-05-06	✓
38	Высокая	CVE-2026-23631	Redis	Сетевой	ACE	2026-05-08	✓
39	Высокая	CVE-2026-23479	Redis	Сетевой	ACE	2026-05-08	✓
40	Высокая	CVE-2026-25243	Redis	Сетевой	ACE	2026-05-08	✓
41	Высокая	CVE-2026-25588	RedisTimeSeries	Сетевой	ACE	2026-05-08	✓
42	Высокая	CVE-2026-25589	RedisBloom	Сетевой	ACE	2026-05-08	✓
43	Высокая	CVE-2026-26129	Microsoft 365 Copilot	Сетевой	OSI	2026-05-12	✓

44	Высокая	CVE-2026-26164	Microsoft 365 Copilot	Сетевой	OSI	2026-05-12	✓
45	Критическая	CVE-2026-0558	LoLLMs	Сетевой	DoS	2026-05-08	✓
46	Высокая	CVE-2026-34330	Windows 10 1607	Локальный	PE	2026-05-13	✓
47	Высокая	CVE-2026-33834	Windows 10 1607	Локальный	SB	2026-05-13	✓
48	Высокая	CVE-2026-35420	Windows Server 2012	Локальный	PE	2026-05-13	✓
49	Высокая	CVE-2026-40369	Windows 11 24H2	Локальный	PE	2026-05-13	✓
50	Высокая	CVE-2026-40382	Windows 10 1607	Локальный	PE	2026-05-13	✓
51	Высокая	CVE-2026-40357	Microsoft SharePoint Server Subscription Edition	Сетевой	ACE	2026-05-13	✓
52	Высокая	CVE-2026-33838	Windows 10 1607	Локальный	PE	2026-05-13	✓
53	Критическая	CVE-2026-42833	Microsoft Dynamics 365	Сетевой	ACE	2026-05-13	✓
54	Высокая	CVE-2026-8264	Tenda AC6	Сетевой	ACE	2026-05-12	✓
55	Высокая	CVE-2026-8260	D-Link DCS-935L	Сетевой	ACE	2026-05-12	✓
56	Высокая	CVE-2026-35415	Windows 10 1607	Локальный	PE	2026-05-13	✓
57	Высокая	CVE-2026-40407	Windows 10 1607	Локальный	PE	2026-05-13	✓
58	Высокая	CVE-2026-33837	Windows 10 1607	Локальный	PE	2026-05-13	✓

59	Высокая	CVE-2026-33841	Windows 10 21H2	Локальный	PE	2026-05-13	✓
60	Высокая	CVE-2026-27886	Data Query Logic in strapi	Сетевой	Не определено	2026-05-13	✓
61	Высокая	CVE-2026-41109	Microsoft GitHub Copilot and Visual Studio Code	Сетевой	OSI	2026-05-13	✓
62	Высокая	CVE-2026-40364	Microsoft Word	Локальный	ACE	2026-05-13	✓
63	Высокая	CVE-2026-40366	Microsoft Word	Локальный	ACE	2026-05-13	✓
64	Высокая	CVE-2026-40361	Microsoft Word	Локальный	ACE	2026-05-13	✓
65	Критическая	CVE-2026-26083	FortiSandbox	Сетевой	ACE	2026-05-13	✓
66	Высокая	CVE-2026-40368	Microsoft SharePoint Server	Сетевой	ACE	2026-05-13	✓
67	Высокая	CVE-2026-35439	Microsoft SharePoint Server	Сетевой	ACE	2026-05-13	✓
68	Высокая	CVE-2026-33110	Microsoft SharePoint Server	Сетевой	ACE	2026-05-13	✓
69	Высокая	CVE-2026-33112	Microsoft SharePoint Server	Сетевой	ACE	2026-05-13	✓
70	Высокая	CVE-2026-40365	Microsoft SharePoint Server	Сетевой	ACE	2026-05-13	✓
71	Критическая	CVE-2026-45185	Exim	Сетевой	ACE	2026-05-13	✓
72	Высокая	CVE-2026-40360	Microsoft Excel	Локальный	OSI	2026-05-13	✓
73	Высокая	CVE-2026-40359	Microsoft Excel	Локальный	ACE	2026-05-13	✓

74	Высокая	CVE-2026-40362	Microsoft Excel	Локальный	ACE	2026-05-13	✓
75	Критическая	CVE-2026-42898	Microsoft Dynamics 365 On-Premises	Сетевой	ACE	2026-05-13	✓
76	Высокая	CVE-2026-42832	Microsoft Office	Локальный	OSI	2026-05-13	✓
77	Высокая	CVE-2026-40363	Microsoft Office	Локальный	ACE	2026-05-13	✓
78	Высокая	CVE-2026-42831	Microsoft Office	Локальный	ACE	2026-05-13	✓
79	Высокая	CVE-2026-40358	Microsoft Office	Локальный	ACE	2026-05-13	✓
80	Высокая	CVE-2026-41094	Microsoft Data Formulator	Сетевой	ACE	2026-05-13	✓
81	Высокая	CVE-2026-34329	Microsoft Message Queuing (MSMQ)	Смежная сеть	ACE	2026-05-13	✓
82	Высокая	CVE-2026-33833	Microsoft Azure Machine Learning Notebook	Сетевой	OSI	2026-05-13	✓
83	Критическая	CVE-2026-41089	Microsoft Windows Netlogon	Сетевой	ACE	2026-05-13	✓
84	Критическая	CVE-2026-33117	Microsoft Azure SDK for Java	Сетевой	SB	2026-05-13	✓
85	Высокая	CVE-2026-40403	Microsoft Windows Graphics Component	Локальный	ACE	2026-05-13	✓
86	Критическая	CVE-2026-41103	Microsoft SSO Plugin for Jira & Confluence	Сетевой	PE	2026-05-13	✓
87	Высокая	CVE-2026-32161	Microsoft Windows Native WiFi Miniport Driver	Смежная сеть	ACE	2026-05-13	✓

88	Высокая	CVE-2026-34332	Microsoft Windows Kernel-Mode Driver	Сетевой	ACE	2026-05-13	✓
89	Высокая	CVE-2026-41611	Microsoft Visual Studio Code	Локальный	XSS\CSS	2026-05-13	✓
90	Высокая	CVE-2026-41613	Microsoft Visual Studio Code	Сетевой	OSI	2026-05-13	✓
91	Критическая	CVE-2026-41096	Microsoft Windows DNS Client	Сетевой	ACE	2026-05-13	✓
92	Высокая	CVE-2026-35438	Microsoft Windows Admin Center	Сетевой	PE	2026-05-13	✓
93	Высокая	CVE-2026-40688	FortiWeb	Сетевой	ACE	2026-04-16	✓
94	Высокая	CVE-2026-0204	SonicWALL SonicOS	Смежная сеть	OSI	2026-04-29	✓

1

Краткое описание: Отказ в обслуживании в OpenClaw

Идентификатор уязвимости: CVE-2026-29609
BDU:2026-06159

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

Уязвимый продукт: OpenClaw: до 2026.2.14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-j27p-hq53-9wgc
- https://github.com/openclaw/openclaw/commit/00a08908892d1743d1fc52e5cbd9499dd5da2fe0
- https://www.vulncheck.com/advisories/openclaw-denial-of-service-via-unbounded-url-backed-media-fetch
- https://bdu.fstec.ru/vul/2026-06159

2

Краткое описание: Отказ в обслуживании в PostgreSQL

Идентификатор уязвимости: BDU:2026-06201

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: PostgreSQL: до 15.14-astra.se2+ci1
Astra Linux Special Edition: 1.8

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

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2025-1202SE17
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2025-1113SE18
- https://wiki.astralinux.ru/astra-linux-se47-bulletin-2025-1216SE47
- https://bdu.fstec.ru/vul/2026-06201

3

Краткое описание: Отказ в обслуживании в Astra Linux Special Edition

Идентификатор уязвимости: BDU:2026-06214

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Astra Linux Special Edition: 4.7
Linux Audit: до 3.0.6

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/linux-audit/audit-userspace/commit/917942329f1a4b1840a59c893c19f496ee7f35ed
- https://github.com/linux-audit/audit-userspace/commit/cd6b9cb6775431be1fb592cff892ad968deddc97
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2025-1202SE17
- https://wiki.astralinux.ru/astra-linux-se47-bulletin-2025-1216SE47
- https://bdu.fstec.ru/vul/2026-06214

Краткое описание: Отказ в обслуживании в libvirt

Идентификатор уязвимости: BDU:2026-06228

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

Уязвимый продукт: libvirt: до 10.5.0-1.astra.se21
Astra Linux Special Edition: 1.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

4

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://gitlab.com/libvirt/libvirt/-/commit/35e3c17e02f5c1bb17ae8a9f2c1b284b3fcbbb90
- https://gitlab.com/libvirt/libvirt/-/work_items/785
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2025-0923SE17
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2025-0811SE18
- https://wiki.astralinux.ru/astra-linux-se47-bulletin-2025-1020SE47
- https://bdu.fstec.ru/vul/2026-06228

5

Краткое описание: Отказ в обслуживании в CUPS

Идентификатор уязвимости: BDU:2026-06252

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: CUPS: до 2.4.11
Astra Linux Special Edition: 3.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/OpenPrinting/cups/issues/1188
- https://github.com/OpenPrinting/cups/pull/1189/changes/7487b879ee5440e2b8313ae17d8f400d3488222e
- https://github.com/OpenPrinting/cups/pull/1189/commits/7487b879ee5440e2b8313ae17d8f400d3488222e
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2025-0923SE17
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2025-0811SE18
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0126SE38
- https://wiki.astralinux.ru/astra-linux-se47-bulletin-2025-1020SE47
- https://bdu.fstec.ru/vul/2026-06252

6

Краткое описание: Отказ в обслуживании в astra-safepolicy

Идентификатор уязвимости: BDU:2026-06276

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: astra-safepolicy: до 3.0+ci111
Astra Linux Special Edition: 3.8

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

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2025-0811SE18
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0126SE38
- https://bdu.fstec.ru/vul/2026-06276

Краткое описание: Выполнение произвольного кода в cPanel

Идентификатор уязвимости: CVE-2026-41940
BDU:2026-06279

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

Уязвимый продукт: cPanel: до 11.136.0.5
WordPress Squared: до 136.1.7
WebHost Manager: до 11.136.0.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

7

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-41940
- https://github.com/watchtowrlabs/watchTowr-vs-cPanel-WHM-AuthBypass-to-RCE.py
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-06279

8

Краткое описание: Выполнение произвольного кода в DIR-605L

Идентификатор уязвимости: CVE-2026-5979
BDU:2026-06280

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

Уязвимый продукт: DIR-605L: 2.13B01 BETA

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/D-Link-DIR-605L-formVirtualServ-33153a41781f80b496e1de206077bc7e
- https://lavender-bicycle-a5a.notion.site/D-Link-DIR-605L-formVirtualServ-33153a41781f80b496e1de206077bc7e?source=copy_link
- https://bdu.fstec.ru/vul/2026-06280

9

Краткое описание: Отказ в обслуживании в Tenda 4G300

Идентификатор уязвимости: CVE-2026-7470
BDU:2026-06160

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda 4G300: 1.01.42_cn_tdc01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/Axelioc/CVE/commit/778e1580b77aa3478a310fe84d08ae14c503ed0e
- https://bdu.fstec.ru/vul/2026-06160

10

Краткое описание: Отказ в обслуживании в Tenda AC9

Идентификатор уязвимости: CVE-2026-6015
BDU:2026-06161

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda AC9: 15.03.02.13

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/Tenda-AC9-QuickIndex-33153a41781f80458940f212f150a4fb
- https://lavender-bicycle-a5a.notion.site/Tenda-AC9-QuickIndex-33153a41781f80458940f212f150a4fb?source=copy_link
- https://bdu.fstec.ru/vul/2026-06161

11

Краткое описание: Отказ в обслуживании в Tenda AC9

Идентификатор уязвимости: CVE-2026-6016
BDU:2026-06163

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda AC9: 15.03.02.13

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/Tenda-AC9-WizardHandle-33153a41781f808480f9e3b78ce438e0
- https://lavender-bicycle-a5a.notion.site/Tenda-AC9-WizardHandle-33153a41781f808480f9e3b78ce438e0?source=copy_link
- https://bdu.fstec.ru/vul/2026-06163

12

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: BDU:2026-06173

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Suricata: от 8.0.0 до 8.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-gr22-4784-xvw3
- https://bdu.fstec.ru/vul/2026-06173

13

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-31935
BDU:2026-06175

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

Уязвимый продукт: Suricata: до 7.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-vxrp-5pg7-7v4x
- https://bdu.fstec.ru/vul/2026-06175

14

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-31934
BDU:2026-06176

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Suricata: от 8.0.0 до 8.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-hr89-h2pp-f3c8
- https://bdu.fstec.ru/vul/2026-06176

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-31933
BDU:2026-06177

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Suricata: до 7.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

15

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-hvp5-gpr6-j4gp
- https://bdu.fstec.ru/vul/2026-06177

16

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-31937
BDU:2026-06178

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Suricata: до 7.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-86vg-w8vm-m3gg
- https://bdu.fstec.ru/vul/2026-06178

17

Краткое описание: Отказ в обслуживании в Suricata

Идентификатор уязвимости: CVE-2026-31932
BDU:2026-06174

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Suricata: до 7.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://github.com/OISF/suricata/security/advisories/GHSA-rp9m-jcpw-hggr
- https://bdu.fstec.ru/vul/2026-06174

18

Краткое описание: Отказ в обслуживании в TOTOLINK N300RH

Идентификатор уязвимости: CVE-2026-7750
BDU:2026-06306

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

Уязвимый продукт: N300RH: 3.2.4-B20220812

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/TOTOLINK-N300RH-setMacFilterRules-34553a41781f809cb952cdcb71ce90d8
- https://vuldb.com/submit/807204
- https://vuldb.com/vuln/360925
- https://bdu.fstec.ru/vul/2026-06306

19

Краткое описание: Выполнение произвольного кода в TOTOLINK N300RH

Идентификатор уязвимости: CVE-2026-7748
BDU:2026-06307

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

Уязвимый продукт: N300RH: 3.2.4-B20220812

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Ссылки на источник:

- https://lavender-bicycle-a5a.notion.site/TOTOLINK-N300RH-setUpgradeFW-34553a41781f80abb1d1c627d7ff4329
- https://vuldb.com/submit/807202
- https://vuldb.com/vuln/360923
- https://bdu.fstec.ru/vul/2026-06307

Краткое описание: Выполнение произвольного кода в D-Link DWR-M960

Идентификатор уязвимости: CVE-2026-2885
BDU:2026-06285

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

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.

20

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/19
- https://bdu.fstec.ru/vul/2026-06285

Краткое описание: Выполнение произвольного кода в D-Link DWR-M960

Идентификатор уязвимости: CVE-2026-2857
BDU:2026-06283

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/14
- https://bdu.fstec.ru/vul/2026-06283

Краткое описание: Выполнение произвольного кода в D-Link DWR-M960

Идентификатор уязвимости: CVE-2026-2856
BDU:2026-06282

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

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.

22

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/13
- https://bdu.fstec.ru/vul/2026-06282

23

Краткое описание: Выполнение произвольного кода в D-Link DWR-M960

Идентификатор уязвимости: CVE-2026-2853
BDU:2026-06281

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DWR-M960: 1.01.07

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/LX-66-LX/cve-new/issues/10
- https://vuldb.com/submit/754456
- https://bdu.fstec.ru/vul/2026-06281

24

Краткое описание: Отказ в обслуживании в DI-8100

Идентификатор уязвимости: CVE-2026-7855
BDU:2026-06338

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

Уязвимый продукт: DI-8100: 16.07.26A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/draw-ctf/report/blob/main/DI-8100/tggl_asp_overflow.md
- https://bdu.fstec.ru/vul/2026-06338

Краткое описание: Выполнение произвольного кода в DI-8100

Идентификатор уязвимости: CVE-2026-7853
BDU:2026-06315

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

Уязвимый продукт: DI-8100: 16.07.26A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

25

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/draw-ctf/report/blob/main/DI-8100/auto_reboot_asp_overflow.md
- https://bdu.fstec.ru/vul/2026-06315

26

Краткое описание: Отказ в обслуживании в DI-8100

Идентификатор уязвимости: CVE-2026-7854
BDU:2026-06316

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

Уязвимый продукт: DI-8100: 16.07.26A1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/draw-ctf/report/blob/main/DI-8100/url_rule_asp_overflow.md
- https://bdu.fstec.ru/vul/2026-06316

Краткое описание: Повышение привилегий в DIR-600L

Идентификатор уязвимости: CVE-2026-42375
BDU:2026-06317

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: DIR-600L: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

27 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://www.securin.io/zero-day/cve-2026-42375-hardcoded-telnet-backdoor-in-d-link-dir-600l-a1-end-of-life-
- https://bdu.fstec.ru/vul/2026-06317

Краткое описание: Повышение привилегий в DIR-456U

Идентификатор уязвимости: CVE-2026-42376
BDU:2026-06321

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: DIR-456U: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

28 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://www.securin.io/zero-day/cve-2026-42376-hardcoded-telnet-backdoor-in-d-link-dir-456u-a1-end-of-life-
- https://bdu.fstec.ru/vul/2026-06321

Краткое описание: Повышение привилегий в DIR-605L

Идентификатор уязвимости: CVE-2026-42372
BDU:2026-06319

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: DIR-605L: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://www.securin.io/zero-day/cve-2026-42372-hardcoded-telnet-backdoor-in-d-link-dir-605l-a1-end-of-life-
- https://bdu.fstec.ru/vul/2026-06319

Краткое описание: Повышение привилегий в DIR-605L

Идентификатор уязвимости: CVE-2026-42373
BDU:2026-06320

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: DIR-605L: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.8 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://www.securin.io/zero-day/cve-2026-42373-hardcoded-telnet-backdoor-in-d-link-dir-605l-b2-end-of-life-
- https://bdu.fstec.ru/vul/2026-06320

Краткое описание: Повышение привилегий в DIR-600L

Идентификатор уязвимости: CVE-2026-42374
BDU:2026-06318

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: DIR-600L: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

31 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://www.securin.io/zero-day/cve-2026-42374-hardcoded-telnet-backdoor-in-d-link-dir-600l-b1-end-of-life-
- https://bdu.fstec.ru/vul/2026-06318

32

Краткое описание: Отказ в обслуживании в Tenda F456

Идентификатор уязвимости: CVE-2026-7032
BDU:2026-06376

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_122/README.md
- https://vuldb.com/submit/798453
- https://vuldb.com/vuln/359612
- https://vuldb.com/vuln/359612/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06376

33

Краткое описание: Выполнение произвольного кода в Tenda F456

Идентификатор уязвимости: CVE-2026-7102
BDU:2026-06375

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_140/README.md
- https://vuldb.com/submit/798475
- https://vuldb.com/vuln/359677
- https://vuldb.com/vuln/359677/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06375

34

Краткое описание: Отказ в обслуживании в Tenda F456

Идентификатор уязвимости: CVE-2026-7078
BDU:2026-06374

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_129/README.md
- https://vuldb.com/submit/798460
- https://vuldb.com/vuln/359653
- https://vuldb.com/vuln/359653/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06374

35

Краткое описание: Выполнение произвольного кода в Tenda F456

Идентификатор уязвимости: CVE-2026-7019
BDU:2026-06373

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_118/README.md
- https://vuldb.com/submit/797473
- https://vuldb.com/vuln/359598
- https://vuldb.com/vuln/359598/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06373

36

Краткое описание: Выполнение произвольного кода в Tenda F456

Идентификатор уязвимости: CVE-2026-7033
BDU:2026-06372

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_123/README.md
- https://vuldb.com/submit/798454
- https://vuldb.com/vuln/359613
- https://vuldb.com/vuln/359613/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06372

37

Краткое описание: Отказ в обслуживании в Tenda F456

Идентификатор уязвимости: CVE-2026-7031
BDU:2026-06377

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

Уязвимый продукт: Tenda F456: 1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_121/README.md
- https://vuldb.com/submit/798452
- https://vuldb.com/vuln/359611
- https://vuldb.com/vuln/359611/cti
- https://www.tenda.com.cn/
- https://bdu.fstec.ru/vul/2026-06377

Краткое описание: Выполнение произвольного кода в Redis

Идентификатор уязвимости: CVE-2026-23631
BDU:2026-06451

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Redis: до 8.6.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

38

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/redis/redis/security/advisories/GHSA-8ghh-qpmp-7826
- https://github.com/redis/redis/releases/tag/8.6.3
- https://github.com/mgiay/CVE-2026-25589-25588-25243-23631-23479-REDIS
- https://bdu.fstec.ru/vul/2026-06451

Краткое описание: Выполнение произвольного кода в Redis

Идентификатор уязвимости: CVE-2026-23479
BDU:2026-06444

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Redis: от 7.2 до 8.6.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

39

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

Ссылки на источник:

- https://github.com/redis/redis/security/advisories/GHSA-93m2-935m-8rj3
- https://github.com/redis/redis/releases/tag/8.6.3
- https://github.com/mgiay/CVE-2026-25589-25588-25243-23631-23479-REDIS
- https://bdu.fstec.ru/vul/2026-06444

Краткое описание: Выполнение произвольного кода в Redis

Идентификатор уязвимости: CVE-2026-25243
BDU:2026-06448

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

Уязвимый продукт: Redis: до 8.6.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

40

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

Ссылки на источник:

- https://github.com/redis/redis/releases/tag/8.6.3
- https://github.com/redis/redis/security/advisories/GHSA-c8h9-259x-jff4
- https://github.com/mgiay/CVE-2026-25589-25588-25243-23631-23479-REDIS
- https://bdu.fstec.ru/vul/2026-06448

Краткое описание: Выполнение произвольного кода в RedisTimeSeries

Идентификатор уязвимости: CVE-2026-25588
BDU:2026-06449

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

Уязвимый продукт: RedisTimeSeries: до 1.12.14

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.

41

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

Ссылки на источник:

- https://github.com/RedisTimeSeries/RedisTimeSeries/security/advisories/GHSA-7jwr-g5qv-w3gw
- https://github.com/RedisTimeSeries/RedisTimeSeries/releases/tag/v1.12.14
- https://github.com/mgiay/CVE-2026-25589-25588-25243-23631-23479-REDIS
- https://bdu.fstec.ru/vul/2026-06449

Краткое описание: Выполнение произвольного кода в RedisBloom

Идентификатор уязвимости: CVE-2026-25589
BDU:2026-06450

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: RedisBloom: до 2.8.20

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.

42

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

Ссылки на источник:

- https://github.com/RedisBloom/RedisBloom/security/advisories/GHSA-7862-34pw-44wv
- https://github.com/RedisBloom/RedisBloom/releases/tag/v2.8.20
- https://github.com/mgiay/CVE-2026-25589-25588-25243-23631-23479-REDIS
- https://bdu.fstec.ru/vul/2026-06450

Краткое описание: Получение конфиденциальной информации в Microsoft 365 Copilot

Идентификатор уязвимости: CVE-2026-26129
BDU:2026-06467

Идентификатор программной ошибки: CWE-138 Некорректная нейтрализация специальных элементов

Уязвимый продукт: Microsoft 365 Copilot: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Получение конфиденциальной информации

43 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26129
- https://bdu.fstec.ru/vul/2026-06467

44

Краткое описание: Получение конфиденциальной информации в Microsoft 365 Copilot

Идентификатор уязвимости: CVE-2026-26164
BDU:2026-06468

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

Уязвимый продукт: Microsoft 365 Copilot: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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.

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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26164
- https://github.com/advisories/GHSA-qvcj-rgrx-wm72
- https://feedly.com/cve/CVE-2026-26164
- https://bdu.fstec.ru/vul/2026-06468

45

Краткое описание: Отказ в обслуживании в LoLLMs

Идентификатор уязвимости: CVE-2026-0558
BDU:2026-06472

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

Уязвимый продукт: LoLLMs: до 2.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://huntr.com/bounties/0a722001-89ce-4c91-b6a6-a55ee5ba2113
- https://github.com/parisneo/lollms/commit/a6625dc83786ff21d109b0d545ca61b770607ef3
- https://bdu.fstec.ru/vul/2026-06472

46

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-34330
BDU:2026-06601

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34330
- https://bdu.fstec.ru/vul/2026-06601

47

Краткое описание: Обход безопасности в Windows 10 1607

Идентификатор уязвимости: CVE-2026-33834
BDU:2026-06603

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33834
- https://bdu.fstec.ru/vul/2026-06603

48

Краткое описание: Повышение привилегий в Windows Server 2012

Идентификатор уязвимости: CVE-2026-35420
BDU:2026-06612

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

Уязвимый продукт: Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35420
- https://feedly.com/cve/CVE-2026-35420
- https://bdu.fstec.ru/vul/2026-06612

Краткое описание: Повышение привилегий в Windows 11 24H2

Идентификатор уязвимости: CVE-2026-40369
BDU:2026-06638

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8390
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

49

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40369
- https://bdu.fstec.ru/vul/2026-06638

50

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40382
BDU:2026-06637

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40382
- https://bdu.fstec.ru/vul/2026-06637

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server Subscription Edition

Идентификатор уязвимости: CVE-2026-40357
BDU:2026-06634

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280
Microsoft SharePoint Enterprise Server 2016: до 16.0.5552.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20128

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

51 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://bdu.fstec.ru/vul/2026-06634

52

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-33838
BDU:2026-06633

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33838
- https://bdu.fstec.ru/vul/2026-06633

53

Краткое описание: Выполнение произвольного кода в Microsoft Dynamics 365

Идентификатор уязвимости: CVE-2026-42833
BDU:2026-06631

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

Уязвимый продукт: Microsoft Dynamics 365: до 9.1.44.15

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42833
- https://feedly.com/cve/CVE-2026-42833
- https://bdu.fstec.ru/vul/2026-06631

54

Краткое описание: Выполнение произвольного кода в Tenda AC6

Идентификатор уязвимости: CVE-2026-8264
BDU:2026-06628

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

Уязвимый продукт: AC6: 15.03.06.23

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://github.com/dxz0069/WAVLINK-WN530H4-Command-Injection-in-set_add_routing/blob/main/Tenda%20AC6V2%20formWifiApScan%20Command%20Injection%20via%20country%20parameter.md
- https://bdu.fstec.ru/vul/2026-06628

Краткое описание: Выполнение произвольного кода в D-Link DCS-935L

Идентификатор уязвимости: CVE-2026-8260
BDU:2026-06625

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

Уязвимый продукт: DCS-935L: до 1.10.01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

55

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://github.com/0xcc12138/DCS-935L-HNAP-Service-CVE
- https://bdu.fstec.ru/vul/2026-06625

56

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-35415
BDU:2026-06617

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://feedly.com/cve/CVE-2026-35415
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35415
- https://bdu.fstec.ru/vul/2026-06617

57

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40407
BDU:2026-06616

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40407
- https://bdu.fstec.ru/vul/2026-06616

58

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-33837
BDU:2026-06632

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33837
- https://bdu.fstec.ru/vul/2026-06632

59

Краткое описание: Повышение привилегий в Windows 10 21H2

Идентификатор уязвимости: CVE-2026-33841
BDU:2026-06739

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

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33841

- https://bdu.fstec.ru/vul/2026-06739

60

Краткое описание: Уязвимость в Data Query Logic in strapi

Идентификатор уязвимости: CVE-2026-27886

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

Уязвимый продукт: strapi: 4.0.0 - 5.36.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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

Оценка CVSSv4: 9.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://github.com/strapi/strapi/security/advisories/GHSA-rjg2-95x7-8qmx

61

Краткое описание: Получение конфиденциальной информации в Microsoft GitHub Copilot and Visual Studio Code

Идентификатор уязвимости: CVE-2026-41109

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

Уязвимый продукт: Visual Studio Code: до 1.119.1

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.8 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41109

62

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-40364

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 16.0.17328.20588
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Word: до 16.0.5552.1000
Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40421
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40366
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40364
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35440
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40367

63

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-40366

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 16.0.17328.20588
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Word: до 16.0.5552.1000
Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40421
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40366
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40364
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35440
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40367

64

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-40361

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 16.0.17328.20588
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Word: до 16.0.5552.1000
Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40421
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40366
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40364
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35440
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40367

Краткое описание: Выполнение произвольного кода в FortiSandbox

Идентификатор уязвимости: CVE-2026-26083

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: FortiSandbox: 4.4.0 - 5.0.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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.

65

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-26-136

66

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-40368

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40368

67

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-35439

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40368

68

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-33110

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40368

69

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-33112

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40368

70

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-40365

Идентификатор программной ошибки: CWE-1220 Недостаточная гранулярность контроля доступа

Уязвимый продукт: Microsoft SharePoint Enterprise Server: до 16.0.5552.1002
Microsoft SharePoint Server: до 16.0.10417.20128
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40357
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40368

71

Краткое описание: Выполнение произвольного кода в Exim

Идентификатор уязвимости: CVE-2026-45185
BDU:2026-06520

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Exim: 4.00 - 4.99.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://exim.org/static/doc/security/EXIM-Security-2026-05-01.1/EXIM-Security-2026-05-01.1.txt
- https://xbow.com/blog/dead-letter-cve-2026-45185-xbow-found-rce-exim
- https://www.openwall.com/lists/oss-security/2026/05/12/4

Краткое описание: Получение конфиденциальной информации в Microsoft Excel

Идентификатор уязвимости: CVE-2026-40360

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Office Online Server : все версии
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: 2016
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40362
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40359
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40360

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-40359

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Office Online Server : все версии
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: 2016
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40362
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40359
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40360

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-40362

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

Уязвимый продукт: Office Online Server : все версии
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: 2016
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40362
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40359
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40360

75

Краткое описание: Выполнение произвольного кода в Microsoft Dynamics 365 On-Premises

Идентификатор уязвимости: CVE-2026-42898

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

Уязвимый продукт: Microsoft Dynamics 365 (on-premises): до 9.1.44.15

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42833
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42898

Краткое описание: Получение конфиденциальной информации в Microsoft Office

Идентификатор уязвимости: CVE-2026-42832

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: 2016 - 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Office for Android: до 16.0.19822.20190
Microsoft Word for Android: до 16.0.19822.20190

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40358
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42831
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40363
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42832

77

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-40363

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: 2016 - 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Office for Android: до 16.0.19822.20190
Microsoft Word for Android: до 16.0.19822.20190

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40358
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42831
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40363
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42832

78

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-42831

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: 2016 - 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Office for Android: до 16.0.19822.20190
Microsoft Word for Android: до 16.0.19822.20190

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40358
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42831
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40363
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42832

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-40358

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: 2016 - 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft Office for Android: до 16.0.19822.20190
Microsoft Word for Android: до 16.0.19822.20190

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

Последствия эксплуатации: Выполнение произвольного кода

79 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40358
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42831
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40363
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42832

80

Краткое описание: Выполнение произвольного кода в Microsoft Data Formulator

Идентификатор уязвимости: CVE-2026-41094

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

Уязвимый продукт: Microsoft Data Formulator: до 0.7

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41094

81

Краткое описание: Выполнение произвольного кода в Microsoft Message Queuing (MSMQ)

Идентификатор уязвимости: CVE-2026-34329

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

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 26H1 10.0.28000.1836
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34329

82

Краткое описание: Получение конфиденциальной информации в Microsoft Azure Machine Learning Notebook

Идентификатор уязвимости: CVE-2026-33833

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

Уязвимый продукт: Azure Machine Learning: до 1.7.6

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33833

83

Краткое описание: Выполнение произвольного кода в Microsoft Windows Netlogon

Идентификатор уязвимости: CVE-2026-41089

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Переполнение буфера.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089

84

Краткое описание: Обход безопасности в Microsoft Azure SDK for Java

Идентификатор уязвимости: CVE-2026-33117

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Azure SDK for Java: до 4.10.6

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33117

85

Краткое описание: Выполнение произвольного кода в Microsoft Windows Graphics Component

Идентификатор уязвимости: CVE-2026-40403

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

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 26H1 10.0.28000.1836
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40403

86

Краткое описание: Повышение привилегий в Microsoft SSO Plugin for Jira & Confluence

Идентификатор уязвимости: CVE-2026-41103

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: Microsoft JIRA SAML SSO plugin: до 1.3.3
Microsoft Confluence SAML SSO plugin: до 7.4.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41103

Краткое описание: Выполнение произвольного кода в Microsoft Windows Native WiFi Miniport Driver

Идентификатор уязвимости: CVE-2026-32161

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

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 26H1 10.0.28000.1836
Windows Server: 2022 10.0.20348.5074 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование ситуации гонки (race condition) в системе.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32161

88

Краткое описание: Выполнение произвольного кода в Microsoft Windows Kernel-Mode Driver

Идентификатор уязвимости: CVE-2026-34332

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server: 2025 10.0.26100.1742 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34332

89

Краткое описание: Межсайтовый скриптинг в Microsoft Visual Studio Code

Идентификатор уязвимости: CVE-2026-41611

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

Уязвимый продукт: Visual Studio Code: 1.0.0 - 14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41613
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41611
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41610

90

Краткое описание: Получение конфиденциальной информации в Microsoft Visual Studio Code

Идентификатор уязвимости: CVE-2026-41613

Идентификатор программной ошибки: CWE-384 Фиксация сессии

Уязвимый продукт: Visual Studio Code: 1.0.0 - 14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.8 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41613
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41611
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41610

91

Краткое описание: Выполнение произвольного кода в Microsoft Windows DNS Client

Идентификатор уязвимости: CVE-2026-41096

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

Уязвимый продукт: Windows: 11 23H2 10.0.22631.1825 - 11 26H1 10.0.28000.1836
Windows Server: 2022 10.0.20348.5074 - 2025 10.0.26100.32690

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданных DNS-запросов.

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41096

92

Краткое описание: Повышение привилегий в Microsoft Windows Admin Center

Идентификатор уязвимости: CVE-2026-35438

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Windows Admin Center: до 2.6.5.16

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35438

93

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2026-40688
BDU:2026-05556

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FortiWeb: от 8.0.0 до 8.0.3 включительно

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 7.2 AV:N/AC:L/PR:H/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: 2026-04-16 / 2026-04-16

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-127
- https://bdu.fstec.ru/vul/2026-05556

94

Краткое описание: Получение конфиденциальной информации в SonicWALL SonicOS

Идентификатор уязвимости: CVE-2026-0204

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

Уязвимый продукт: Gen6 Hardware Firewalls -SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650,NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250,SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W: до 6.5.5.2-28n
Gen7 NSv - NSv 270, NSv 470, NSv 870. Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W,TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700. Gen7 NSv - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure): до 7.3.2-7010
Gen8 Firewalls - TZ80, TZ280, TZ280W, TZ380, TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800: до 8.2.0-8009

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-05-05

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-0204
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004