НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-07-01.1 | 1 июля 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-34986	Red Hat OpenShift Container Platform 4.22	Сетевой	DoS	2026-06-16	✔
2	Критическая	CVE-2026-32267	Craft CMS	Сетевой	PE	2026-06-16	✔
3	Высокая	CVE-2026-54420	LiteSpeed User-End cPanel Plugin	Сетевой	PE	2026-06-16	✔
4	Высокая	CVE-2026-12057	Foxit AI	Локальный	ACE	2026-06-16	✔
5	Высокая	CVE-2026-44741	Pimcore admin-ui-classic-bundle	Сетевой	OSI	2026-06-15	✔
6	Высокая	CVE-2026-11799	Mozilla Focus for iOS	Сетевой	XSS\CSS	2026-06-15	✔
7	Высокая	CVE-2026-54271	protobufjs-cli	Сетевой	ACE	2026-06-13	✔
8	Высокая	CVE-2026-47292	Microsoft Visual Studio Code MSSQL Extension	Локальный	ACE	2026-06-12	✔
9	Высокая	CVE-2026-45591	Microsoft ASP.NET Core	Сетевой	DoS	2026-06-12	✔
10	Высокая	CVE-2026-45636	Microsoft Windows NTFS	Локальный	ACE	2026-06-12	✔
11	Критическая	CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools	Сетевой	ACE	2026-06-12	✔
12	Критическая	CVE-2026-33186	Red Hat OpenShift Container Platform 4.19	Сетевой	SB	2026-06-10	✔

13	Высокая	CVE-2026-46306	Linux kernel core	Сетевой	DoS	2026-06-10	✔
14	Высокая	CVE-2026-40371	Microsoft Dynamics 365 (on-premises)	Сетевой	PE	2026-06-10	✔
15	Высокая	BDU:2026-08016	Visual Studio Code	Сетевой	XSS\CSS	2026-06-09	✔
16	Высокая	CVE-2026-36816	Tenda W15E	Сетевой	DoS	2026-06-10	✔
17	Высокая	CVE-2026-36817	Tenda W15E	Сетевой	DoS	2026-06-10	✔
18	Высокая	CVE-2026-36818	Tenda W15E	Сетевой	DoS	2026-06-10	✔
19	Высокая	CVE-2026-36819	Tenda W15E	Сетевой	DoS	2026-06-10	✔
20	Высокая	CVE-2026-36820	Tenda W15E	Сетевой	DoS	2026-06-10	✔
21	Высокая	CVE-2026-36821	Tenda W15E	Сетевой	DoS	2026-06-10	✔
22	Высокая	CVE-2026-36822	Tenda W15E	Сетевой	DoS	2026-06-10	✔
23	Высокая	CVE-2026-36823	Tenda W15E	Сетевой	DoS	2026-06-10	✔
24	Высокая	CVE-2026-36815	Tenda W15E	Сетевой	DoS	2026-06-10	✔
25	Высокая	CVE-2026-42501	Go	Сетевой	SB	2026-06-10	✔
26	Высокая	CVE-2026-49160	Windows	Сетевой	DoS	2026-06-10	✔
27	Высокая	CVE-2026-45186	libexpat	Сетевой	DoS	2026-06-10	✔

28	Высокая	CVE-2026-34696	Adobe InDesign	Локальный	ACE	2026-06-10	✔
29	Высокая	CVE-2026-34698	Adobe InDesign	Локальный	ACE	2026-06-10	✔
30	Высокая	CVE-2026-34699	Adobe InDesign	Локальный	ACE	2026-06-10	✔
31	Высокая	CVE-2026-34695	Adobe InDesign	Локальный	ACE	2026-06-10	✔
32	Высокая	CVE-2026-34701	Adobe InDesign	Локальный	ACE	2026-06-10	✔
33	Высокая	CVE-2026-34702	Adobe InDesign	Локальный	ACE	2026-06-10	✔
34	Высокая	CVE-2026-45586	Windows	Локальный	PE	2026-06-10	✔
35	Высокая	CVE-2026-36813	Tenda W15E	Сетевой	DoS	2026-06-10	✔
36	Высокая	CVE-2026-34697	Adobe InDesign	Локальный	ACE	2026-06-10	✔
37	Высокая	CVE-2026-36810	Tenda W15E	Сетевой	DoS	2026-06-10	✔
38	Высокая	CVE-2026-36811	Tenda W15E	Сетевой	DoS	2026-06-10	✔
39	Высокая	BDU:2026-08019	Windows	Локальный	PE	2026-06-10	✔
40	Высокая	CVE-2026-44113	OpenClaw	Сетевой	SB	2026-06-09	✔
41	Высокая	CVE-2026-44118	OpenClaw	Локальный	SB	2026-06-09	✔
42	Критическая	CVE-2026-44112	OpenClaw	Сетевой	ACE	2026-06-09	✔

43	Высокая	CVE-2026-44115	OpenClaw	Сетевой	ACE	2026-06-09	✔
44	Критическая	CVE-2026-42248	Ollama	Сетевой	ACE	2026-06-09	✔
45	Критическая	CVE-2026-42249	Ollama	Сетевой	ACE	2026-06-09	✔
46	Критическая	CVE-2026-7482	Ollama	Сетевой	OSI	2026-06-09	✔
47	Критическая	CVE-2026-10520	Ivanti Sentry	Сетевой	ACE	2026-06-10	✔
48	Высокая	CVE-2026-23111	Linux	Локальный	DoS	2026-06-10	✔
49	Высокая	CVE-2026-11003	Google Chrome	Сетевой	ACE	2026-06-10	✔
50	Критическая	CVE-2026-11043	Google Chrome	Сетевой	SB	2026-06-10	✔
51	Высокая	CVE-2026-11012	Google Chrome	Сетевой	SB	2026-06-10	✔
52	Критическая	CVE-2026-11009	Google Chrome	Сетевой	SB	2026-06-10	✔
53	Высокая	CVE-2026-36806	Tenda W15E	Сетевой	DoS	2026-06-10	✔
54	Высокая	CVE-2026-36807	Tenda W15E	Сетевой	DoS	2026-06-10	✔
55	Высокая	CVE-2026-36808	Tenda W15E	Сетевой	DoS	2026-06-10	✔
56	Высокая	CVE-2026-11645	Google Chrome	Сетевой	ACE	2026-06-09	✔
57	Высокая	CVE-2026-36809	Tenda W15E	Сетевой	DoS	2026-06-10	✔

58	Высокая	CVE-2026-42985	Windows	Сетевой	ACE	2026-06-10	✔
59	Высокая	CVE-2026-44801	Windows	Сетевой	ACE	2026-06-10	✔
60	Высокая	CVE-2026-45458	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-06-10	✔
61	Высокая	CVE-2026-47654	Windows Server	Сетевой	ACE	2026-06-10	✔
62	Высокая	CVE-2026-47652	Windows	Локальный	ACE	2026-06-10	✔
63	Критическая	CVE-2026-47291	Windows	Сетевой	ACE	2026-06-10	✔
64	Критическая	CVE-2026-45657	Windows	Сетевой	ACE	2026-06-10	✔
65	Высокая	CVE-2026-47635	Microsoft Office LTSC 2024	Локальный	ACE	2026-06-10	✔
66	Высокая	CVE-2026-48574	Windows	Локальный	ACE	2026-06-10	✔
67	Высокая	CVE-2026-45476	Linux kernel - Microsoft MANA Network Driver	Локальный	PE	2026-06-10	✔
68	Высокая	CVE-2026-45463	Microsoft Office	Локальный	ACE	2026-06-10	✔
69	Критическая	CVE-2026-26142	Microsoft Office	Сетевой	ACE	2026-06-10	✔
70	Высокая	CVE-2026-47289	Windows	Сетевой	ACE	2026-06-10	✔
71	Высокая	CVE-2026-47911	Adobe Reader	Локальный	ACE	2026-06-11	✔
72	Высокая	CVE-2026-47914	Adobe Reader	Локальный	ACE	2026-06-11	✔

73	Высокая	CVE-2026-47915	Adobe Reader	Локальный	ACE	2026-06-11	✔
74	Высокая	CVE-2026-47916	Adobe Reader	Локальный	ACE	2026-06-11	✔
75	Высокая	CVE-2026-47959	Adobe Reader	Локальный	ACE	2026-06-11	✔
76	Высокая	CVE-2026-47917	Adobe Reader	Локальный	ACE	2026-06-11	✔
77	Высокая	CVE-2026-47918	Adobe Reader	Локальный	ACE	2026-06-11	✔
78	Высокая	CVE-2026-47920	Adobe Reader	Локальный	ACE	2026-06-11	✔
79	Высокая	CVE-2026-47955	Adobe Reader	Локальный	ACE	2026-06-11	✔

1

Краткое описание: Отказ в обслуживании в Red Hat OpenShift Container Platform 4.22

Идентификатор уязвимости: CVE-2026-34986

Идентификатор программной ошибки: CWE-248 Необработанное исключение

Уязвимый продукт: Red Hat OpenShift Container Platform: до 4.22.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:25206

2

Краткое описание: Повышение привилегий в Craft CMS

Идентификатор уязвимости: CVE-2026-32267

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Craft CMS: 4.0.0 - 5.9.11

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: 7.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://github.com/craftcms/cms/security/advisories/GHSA-cc7p-2j3x-x7xf
- https://github.com/craftcms/cms/commit/6301e217c5f15617d939c432cb770db50af14b33

3

Краткое описание: Повышение привилегий в LiteSpeed User-End cPanel Plugin

Идентификатор уязвимости: CVE-2026-54420

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

Уязвимый продукт: LiteSpeed User-End cPanel Plugin: до 2.4.8
LiteSpeed WHM Plugin: до 5.3.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/

4

Краткое описание: Выполнение произвольного кода в Foxit AI

Идентификатор уязвимости: CVE-2026-12057

Идентификатор программной ошибки: CWE-829 Использование функций недоверенных источников

Уязвимый продукт: Foxit AI: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного PDF-файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Foxit+AI+security+update2026-06-15+00%3A00%3A00

5

Краткое описание: Получение конфиденциальной информации в Pimcore admin-ui-classic-bundle

Идентификатор уязвимости: CVE-2026-44741

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Pimcore admin-ui-classic-bundle: 2.0.0 - 2.3.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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:L/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/pimcore/pimcore/security/advisories/GHSA-h4ph-crvj-9h92

6

Краткое описание: Межсайтовый скриптинг в Mozilla Focus for iOS

Идентификатор уязвимости: CVE-2026-11799

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

Уязвимый продукт: Focus for iOS: до 151.3.1

Категория уязвимого продукта: Мобильные платформы

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-55/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1975667

7

Краткое описание: Выполнение произвольного кода в protobufjs-cli

Идентификатор уязвимости: CVE-2026-54271

Идентификатор программной ошибки: Не определено

Уязвимый продукт: protobufjs-cli: 1.0.0 - 2.4.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-13 / 2026-06-13

Ссылки на источник:

- https://github.com/protobufjs/protobuf.js/security/advisories/GHSA-pr59-h9ph-3fr8

8

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio Code MSSQL Extension

Идентификатор уязвимости: CVE-2026-47292
BDU:2026-08317

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

Уязвимый продукт: Visual Studio Code - MSSQL Extension: до 1.123.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-12 / 2026-06-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47292

9

Краткое описание: Отказ в обслуживании в Microsoft ASP.NET Core

Идентификатор уязвимости: CVE-2026-45591

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

Уязвимый продукт: .NET for Linux: 8.0.0 - 9.0.16
.NET for macOS: 8.0.0 - 9.0.16
ASP.NET Core: 8.0 - 9.0.16
.NET: 8.0.0 - 9.0.16
Microsoft .NET Framework: до 10.0.9

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-12 / 2026-06-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45591

10

Краткое описание: Выполнение произвольного кода в Microsoft Windows NTFS

Идентификатор уязвимости: CVE-2026-45636
BDU:2026-08284

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 21H2 10.0.19044.7291 - 11 26H1 10.0.28000.1836
Windows Server: 2012 6.2.9200.26079 - 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: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-12 / 2026-06-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45636

Краткое описание: Выполнение произвольного кода в Oracle PeopleSoft Enterprise PeopleTools

Идентификатор уязвимости: CVE-2026-35273
BDU:2026-08250

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

Уязвимый продукт: PeopleSoft Enterprise PeopleTools: 8.61, 8.62

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-12 / 2026-06-12

Ссылки на источник:

- https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

Краткое описание: Обход безопасности в Red Hat OpenShift Container Platform 4.19

Идентификатор уязвимости: CVE-2026-33186
BDU:2026-04598

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Red Hat OpenShift Container Platform: до 4.19.33

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:23247

Краткое описание: Отказ в обслуживании в Linux kernel core

Идентификатор уязвимости: CVE-2026-46306

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Linux kernel: 7.0 rc1, 7.0 rc2

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

Способ эксплуатации: Не определено

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

1
3

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/stable/c/0d00b9015069712944934bab09eaa6c542143049
- https://git.kernel.org/stable/c/18ae9eacfc95cc715c0606b2c86e8aa8a86cf3e3
- https://git.kernel.org/stable/c/6044392d9cace3a3672b02c8bc7d38b502e51734
- https://git.kernel.org/stable/c/7c93f353eab4ea911e394630f07d72e040a729d8
- https://git.kernel.org/stable/c/abc5bc84e0f2edc7ea2d437afa6ef3fe1fc43200
- https://git.kernel.org/stable/c/d6c19b31a3c1d519fabdcf0aa239e6b6109b9473
- https://git.kernel.org/stable/c/db104b0d8a7856397c0469d83a4289adf7c54863
- https://git.kernel.org/stable/c/e7c811ca372d53c2be7d01a1614e71fae1054836

Краткое описание: Повышение привилегий в Microsoft Dynamics 365 (on-premises)

Идентификатор уязвимости: CVE-2026-40371
BDU:2026-08299

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Microsoft Dynamics 365 (on-premises): до 9.1 Train 26062 06.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40371

15

Краткое описание: Межсайтовый скриптинг в Visual Studio Code

Идентификатор уязвимости: BDU:2026-08016

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

Уязвимый продукт: Visual Studio Code: от 1.97 до 1.124.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://blog.ammaraskar.com/github-token-stealing/
- https://github.com/microsoft/vscode/issues/319593
- https://bdu.fstec.ru/vul/2026-08016

16

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36816
BDU:2026-08052

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formAddWewifiWhiteUser
- https://bdu.fstec.ru/vul/2026-08052

17

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36817
BDU:2026-08053

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formAddWebAuthWhiteUser
- https://bdu.fstec.ru/vul/2026-08053

18

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36818
BDU:2026-08054

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/formAddWewifiWhiteUser
- https://bdu.fstec.ru/vul/2026-08054

19

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36819
BDU:2026-08055

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/fromSetDhcpRules
- https://bdu.fstec.ru/vul/2026-08055

20

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36820
BDU:2026-08056

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/formAddWebAuthWhiteUser
- https://bdu.fstec.ru/vul/2026-08056

21

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36821
BDU:2026-08057

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/formCropAndSetWewifiPic
- https://bdu.fstec.ru/vul/2026-08057

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36822
BDU:2026-08058

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/formDelStaState
- https://bdu.fstec.ru/vul/2026-08058

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36823
BDU:2026-08059

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W20E/formAddWebAuthUser
- https://bdu.fstec.ru/vul/2026-08059

2
3

24

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36815
BDU:2026-08051

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formSetNetCheckTools
- https://bdu.fstec.ru/vul/2026-08051

Краткое описание: Обход безопасности в Go

Идентификатор уязвимости: CVE-2026-42501
BDU:2026-08061

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Go: от 1.26.0 до 1.26.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

25

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://go.dev/cl/775321
- https://go.dev/issue/79070
- https://groups.google.com/g/golang-announce/c/qcCIEXso47M
- https://pkg.go.dev/vuln/GO-2026-4984
- https://bdu.fstec.ru/vul/2026-08061

26

Краткое описание: Отказ в обслуживании в Windows

Идентификатор уязвимости: CVE-2026-49160
BDU:2026-08063

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49160
- https://bdu.fstec.ru/vul/2026-08063

Краткое описание: Отказ в обслуживании в libexpat

Идентификатор уязвимости: CVE-2026-45186
BDU:2026-08066

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: libexpat: до 2.8.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/05/11/16
- https://github.com/libexpat/libexpat/pull/1216
- https://bdu.fstec.ru/vul/2026-08066

28

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34696
BDU:2026-08067

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08067

29

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34698
BDU:2026-08069

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

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08069

30

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34699
BDU:2026-08070

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

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08070

31

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34695
BDU:2026-08071

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08071

32

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34701
BDU:2026-08072

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

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08072

33

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34702
BDU:2026-08073

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08073

34

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2026-45586
BDU:2026-08062

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45586
- https://bdu.fstec.ru/vul/2026-08062

35

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36813
BDU:2026-08050

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formCropAndSetWewifiPic
- https://bdu.fstec.ru/vul/2026-08050

36

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-34697
BDU:2026-08068

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe InDesign: до 20.5.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-58.html
- https://bdu.fstec.ru/vul/2026-08068

37

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36810
BDU:2026-08048

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formPortalAuth
- https://bdu.fstec.ru/vul/2026-08048

38

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36811
BDU:2026-08049

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formDelwebAuthPic
- https://bdu.fstec.ru/vul/2026-08049

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: BDU:2026-08019

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

Уязвимый продукт: Windows 10: -
Windows 11: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/MSNightmare/RoguePlanet
- https://bdu.fstec.ru/vul/2026-08019

Краткое описание: Обход безопасности в OpenClaw

Идентификатор уязвимости: CVE-2026-44113
BDU:2026-08022

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: OpenClaw: до 2026.4.21 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

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.

40

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-5h3g-6xhh-rg6p
- https://github.com/openclaw/openclaw/commit/95119017c847c737bd113f0bff728c4666d79c45
- https://bdu.fstec.ru/vul/2026-08022

Краткое описание: Обход безопасности в OpenClaw

Идентификатор уязвимости: CVE-2026-44118
BDU:2026-08023

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

Уязвимый продукт: OpenClaw: до 2026.4.21 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

41

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-r6xh-pqhr-v4xh
- https://github.com/openclaw/openclaw/commit/3cb1a56bfc9579a0f2336f9cfa12a8a744332a19
- https://bdu.fstec.ru/vul/2026-08023

Краткое описание: Выполнение произвольного кода в OpenClaw

Идентификатор уязвимости: CVE-2026-44112
BDU:2026-08024

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: OpenClaw: до 2026.4.21 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

42

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-wppj-c6mr-83jj
- https://github.com/openclaw/openclaw/commit/7be82d4fd1193bcb7e44ee38838f00bf924ffa76
- https://bdu.fstec.ru/vul/2026-08024

Краткое описание: Выполнение произвольного кода в OpenClaw

Идентификатор уязвимости: CVE-2026-44115
BDU:2026-08025

Идентификатор программной ошибки: CWE-184 Неполный черный список

Уязвимый продукт: OpenClaw: до 2026.4.21 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

43

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/openclaw/openclaw/security/advisories/GHSA-x3h8-jrgh-p8jx
- https://github.com/openclaw/openclaw/commit/b2e8b7d4bb2f22eaa16f5c4b07547774e90b65a5
- https://bdu.fstec.ru/vul/2026-08025

Краткое описание: Выполнение произвольного кода в Ollama

Идентификатор уязвимости: CVE-2026-42248
BDU:2026-08026

Идентификатор программной ошибки: CWE-494 Загрузка кода без проверки его целостности

Уязвимый продукт: Ollama: от 0.12.10 до 0.17.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://cert.pl/en/posts/2026/04/CVE-2026-42248/
- https://ollama.com/
- https://bdu.fstec.ru/vul/2026-08026

Краткое описание: Выполнение произвольного кода в Ollama

Идентификатор уязвимости: CVE-2026-42249
BDU:2026-08027

Идентификатор программной ошибки: CWE-494 Загрузка кода без проверки его целостности

Уязвимый продукт: Ollama: от 0.12.10 до 0.17.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://cert.pl/en/posts/2026/04/CVE-2026-42248/
- https://ollama.com/
- https://bdu.fstec.ru/vul/2026-08027

Краткое описание: Получение конфиденциальной информации в Ollama

Идентификатор уязвимости: CVE-2026-7482
BDU:2026-08028

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Ollama: до 0.17.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

4
6

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/ollama/ollama/commit/88d57d0483cca907e0b23a968c83627a20b21047
- https://github.com/ollama/ollama/pull/14406
- https://github.com/ollama/ollama/releases/tag/v0.17.1
- https://bdu.fstec.ru/vul/2026-08028

Краткое описание: Выполнение произвольного кода в Ivanti Sentry

Идентификатор уязвимости: CVE-2026-10520
BDU:2026-08029

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

Уязвимый продукт: Ivanti Sentry: до 10.7.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

4
7

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523
- https://labs.watchtowr.com/more-evidence-that-words-dont-mean-what-we-thought-they-meant-ivanti-sentry-pre-auth-os-command-injection-cve-2026-10520/
- https://www.bleepingcomputer.com/news/security/new-max-severity-ivanti-sentry-flaw-allows-code-execution-as-root/
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-08029

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-23111
BDU:2026-08031

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: до 6.3.10
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 25.10
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

4
8

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://securityaffairs.com/193352/hacking/cve-2026-23111-linux-nf_tables-flaw-enables-root-exploits.html
- https://blog.exodusintel.com/2026/06/08/off-by-exploiting-a-use-after-free-in-the-linux-kernel/
- https://git.kernel.org/stable/c/1444ff890b4653add12f734ffeffc173d42862dd
- https://git.kernel.org/stable/c/42c574c1504aa089a0a142e4c13859327570473d
- https://git.kernel.org/stable/c/8b68a45f9722f2babe9e7bad00aa74638addf081
- https://git.kernel.org/stable/c/8c760ba4e36c750379d13569f23f5a6e185333f5
- https://git.kernel.org/stable/c/b9b6573421de51829f7ec1cce76d85f5f6fbbd7f
- https://git.kernel.org/stable/c/f41c5d151078c5348271ffaf8e7410d96f2d82f8

- https://access.redhat.com/security/cve/cve-2026-23111
- https://security-tracker.debian.org/tracker/CVE-2026-23111
- https://ubuntu.com/security/CVE-2026-23111
- https://bdu.fstec.ru/vul/2026-08031

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11003
BDU:2026-08036

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

4
9

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11003
- https://bdu.fstec.ru/vul/2026-08036

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11043
BDU:2026-08039

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 149.0.7827.53
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11043
- https://bdu.fstec.ru/vul/2026-08039

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11012
BDU:2026-08040

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

5
1

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11012
- https://bdu.fstec.ru/vul/2026-08040

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11009
BDU:2026-08041

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11009
- https://bdu.fstec.ru/vul/2026-08041

5
2

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36806
BDU:2026-08044

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

Уязвимый продукт: Tenda W15E: 15.11.0.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Отказ в обслуживании

5
3 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formModifyWebAuthUser
- https://bdu.fstec.ru/vul/2026-08044

54

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36807
BDU:2026-08045

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formAddWebAuthUser
- https://bdu.fstec.ru/vul/2026-08045

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36808
BDU:2026-08046

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formAddWebAuthUser
- https://bdu.fstec.ru/vul/2026-08046

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11645
BDU:2026-08030

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-08030

Краткое описание: Отказ в обслуживании в Tenda W15E

Идентификатор уязвимости: CVE-2026-36809
BDU:2026-08047

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenda W15E: 15.11.0.10

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

Ссылки на источник:

- https://github.com/xhh0124/SemVulLLM/tree/main/W15E/formModifyWebAuthWhiteUser
- https://bdu.fstec.ru/vul/2026-08047

58

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-42985
BDU:2026-08107

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Remote Desktop client for Windows Desktop: до 1.2.7214.0
Windows App Client for Windows Desktop: до 2.0.1193.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

только после оценки всех сопутствующих рисков.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42985
- https://bdu.fstec.ru/vul/2026-08107

59

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-44801
BDU:2026-08108

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269
Remote Desktop client for Windows Desktop: до 1.2.7214.0
Windows App Client for Windows Desktop: до 2.0.1193.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44801
- https://bdu.fstec.ru/vul/2026-08108

60

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

Идентификатор уязвимости: CVE-2026-45458
BDU:2026-08109

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20384
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -

Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5556.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5556.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20153
Microsoft Office 365: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45458
- https://bdu.fstec.ru/vul/2026-08109

61

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2026-47654
BDU:2026-08110

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47654
- https://bdu.fstec.ru/vul/2026-08110

62

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-47652
BDU:2026-08111

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

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47652
- https://bdu.fstec.ru/vul/2026-08111

63

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-47291
BDU:2026-08115

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

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47291
- https://bdu.fstec.ru/vul/2026-08115

6	**Краткое описание:** Выполнение произвольного кода в Windows

4

Идентификатор уязвимости: CVE-2026-45657
BDU:2026-08113

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45657
- https://bdu.fstec.ru/vul/2026-08113

6
5

Краткое описание: Выполнение произвольного кода в Microsoft Office LTSC 2024

Идентификатор уязвимости: CVE-2026-47635

BDU:2026-08114

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

Уязвимый продукт: Microsoft Office LTSC 2024: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47635
- https://bdu.fstec.ru/vul/2026-08114

6
6

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-48574

BDU:2026-08106

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48574
- https://bdu.fstec.ru/vul/2026-08106

67

Краткое описание: Повышение привилегий в Linux kernel - Microsoft MANA Network Driver

Идентификатор уязвимости: CVE-2026-45476
BDU:2026-08116

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux kernel - Microsoft MANA Network Driver: до 7.1

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45476
- https://bdu.fstec.ru/vul/2026-08116

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-45463
BDU:2026-08117

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

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45463
- https://bdu.fstec.ru/vul/2026-08117

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-26142
BDU:2026-08118

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

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

Категория уязвимого продукта: Прикладное программное обеспечение

6
9

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26142
- https://bdu.fstec.ru/vul/2026-08118

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2026-47289
BDU:2026-08112

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

7
0

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47289
- https://bdu.fstec.ru/vul/2026-08112

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47911
BDU:2026-08105

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

71

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08105

7
2

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47914
BDU:2026-08097

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08097

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47915
BDU:2026-08101

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
3

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08101

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47916
BDU:2026-08100

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
4

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08100

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47959
BDU:2026-08098

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
5

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08098

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47917
BDU:2026-08096

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
6

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08096

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47918
BDU:2026-08095

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
7

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08095

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47920
BDU:2026-08094

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
8

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08094

Краткое описание: Выполнение произвольного кода в Adobe Reader

Идентификатор уязвимости: CVE-2026-47955
BDU:2026-08092

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

7
9

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html
- https://bdu.fstec.ru/vul/2026-08092