НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-07-30.1 | 30 июля 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2025-8044	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
2	Критическая	CVE-2025-8028	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
3	Высокая	CVE-2025-8029	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
4	Высокая	CVE-2025-8036	Mozilla Firefox	Сетевой	SB	2025-07-22	✓
5	Критическая	CVE-2025-8037	Mozilla Firefox	Сетевой	SB	2025-07-22	✓
6	Высокая	CVE-2025-8030	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
7	Критическая	CVE-2025-8031	Mozilla Firefox	Сетевой	OSI	2025-07-22	✓
8	Критическая	CVE-2025-8038	Mozilla Firefox	Сетевой	SB	2025-07-22	✓
9	Высокая	CVE-2025-8039	Mozilla Firefox	Сетевой	OSI	2025-07-22	✓
10	Высокая	CVE-2025-8034	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
11	Высокая	CVE-2025-8040	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
12	Высокая	CVE-2025-8035	Mozilla Firefox	Сетевой	ACE	2025-07-22	✓
13	Высокая	CVE-2025-8032	Mozilla Firefox	Сетевой	SB	2025-07-22	✓

14	Высокая	CVE-2023-44487	Schneider Electric EcoStruxure Power Operation	Сетевой	DoS	2025-07-23	✓
15	Высокая	CVE-2023-35945	Schneider Electric EcoStruxure Power Operation	Сетевой	DoS	2025-07-23	✓
16	Высокая	CVE-2022-45198	Schneider Electric EcoStruxure Power Operation	Сетевой	DoS	2025-07-23	✓
17	Высокая	CVE-2023-50447	Schneider Electric EcoStruxure Power Operation	Сетевой	ACE	2025-07-23	✓
18	Критическая	CVE-2022-22817	Schneider Electric EcoStruxure Power Operation	Сетевой	OSI	2025-07-23	✓
19	Критическая	CVE-2025-54309	CrushFTP	Сетевой	SB	2025-07-21	✓
20	Критическая	CVE-2025-53770	Microsoft SharePoint Server	Сетевой	ACE	2025-07-20	✓
21	Высокая	CVE-2025-5039	Autodesk Desktop products	Локальный	ACE	2025-07-28	✓
22	Критическая	CVE-2024-20148	Leovo MediaTek WLAN driver	Сетевой	ACE	2025-07-28	✓
23	Высокая	CVE-2025-8011	Microsoft Edge	Сетевой	ACE	2025-07-28	✓
24	Высокая	CVE-2025-8010	Microsoft Edge	Сетевой	ACE	2025-07-28	✓
25	Высокая	CVE-2025-3947	Honeywell Experion PKS	Сетевой	DoS	2025-07-25	✓
26	Высокая	CVE-2025-3946	Honeywell Experion PKS	Сетевой	ACE	2025-07-25	✓
27	Критическая	CVE-2025-2523	Honeywell Experion PKS	Сетевой	ACE	2025-07-25	✓

28	Высокая	CVE-2025-2521	Honeywell Experion PKS	Сетевой	ACE	2025-07-25	✓
29	Высокая	CVE-2025-2520	Honeywell Experion PKS	Сетевой	DoS	2025-07-25	✓
30	Высокая	CVE-2025-7656	Google ChromeOS	Сетевой	ACE	2025-07-24	✓
31	Высокая	CVE-2025-6558	Google ChromeOS	Сетевой	OSI	2025-07-24	✓
32	Высокая	CVE-2025-7657	Google ChromeOS	Сетевой	ACE	2025-07-24	✓
33	Критическая	CVE-2025-40599	SonicWall SMA100 SSL-VPN	Сетевой	WLF	2025-07-23	✓
34	Высокая	CVE-2025-40597	SonicWall SMA100 SSL-VPN	Сетевой	ACE	2025-07-23	✓
35	Высокая	CVE-2025-31701	Dahua products	Сетевой	ACE	2025-07-23	✓
36	Высокая	CVE-2025-31700	Dahua products	Сетевой	ACE	2025-07-23	✓
37	Высокая	CVE-2025-34057	Ruijie NBR	Сетевой	ACE	2025-07-02	✗
38	Критическая	CVE-2025-25257	FortiWeb	Сетевой	ACE	2025-07-08	✓
39	Высокая	CVE-2025-7656	Microsoft Edge	Сетевой	ACE	2025-07-17	✓
40	Высокая	CVE-2025-6558	Microsoft Edge	Сетевой	OSI	2025-07-17	✓
41	Высокая	CVE-2025-7657	Microsoft Edge	Сетевой	ACE	2025-07-17	✓
42	Критическая	CVE-2025-41238	VMware products	Локальный	ACE	2025-07-17	✓

43	Критическая	CVE-2025-41237	VMware products	Локальный	ACE	2025-07-17	✓
44	Критическая	CVE-2025-41236	VMware products	Локальный	ACE	2025-07-17	✓
45	Высокая	CVE-2025-24928	Oracle HTTP Server	Локальный	ACE	2025-07-16	✓
46	Высокая	CVE-2024-38477	Oracle HTTP Server	Сетевой	DoS	2025-07-16	✓
47	Высокая	CVE-2024-8176	Oracle HTTP Server	Сетевой	ACE	2025-07-16	✓
48	Высокая	CVE-2025-50059	Oracle Java SE	Сетевой	OSI	2025-07-16	✓
49	Высокая	CVE-2025-30749	Oracle Java SE	Сетевой	ACE	2025-07-16	✓
50	Высокая	CVE-2025-50106	Oracle Java SE	Сетевой	ACE	2025-07-16	✓
51	Высокая	CVE-2025-24855	Oracle Java SE	Локальный	ACE	2025-07-16	✓

1

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8044

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

Уязвимый продукт: Mozilla Firefox: 140.0 - 140.0.4
Firefox for Android: 140.0 - 140.0.4

Категория уязвимого продукта: Не определено

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/

2

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8028
BDU:2025-08995

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: Mozilla Firefox: 120.0 - 140.0.4
Firefox ESR: 115.0 - 140.0
Firefox for Android: 120.0 - 140.0.4

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 4.8 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1971581
- https://bdu.fstec.ru/vul/2025-08995

3

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8029

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1928021

4

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8036

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1960834

5

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8037

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

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: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1964767

6

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8030

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 1.2 AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1968414

7

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8031

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 0.5 AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1971719

8

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8038

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

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

Оценка CVSSv4: 0.5 AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1808979

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8039

Идентификатор программной ошибки: CWE-450 Наличие вариантов интерпретации входных данных интерфейсом

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv4: 0.5 AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1970997

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8034

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

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

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.

10

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8040

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

11 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8035

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

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

12

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-8032

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Firefox: 128.0 - 140.0.4
Firefox ESR: 128.0 - 140.0
Firefox for Android: 128.0 - 140.0.4
Mozilla Thunderbird: 130.0 - 139.0.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-22 / 2025-07-22

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1974407

Краткое описание: Отказ в обслуживании в Schneider Electric EcoStruxure Power Operation

Идентификатор уязвимости: CVE-2023-44487
BDU:2023-06559

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

Уязвимый продукт: EcoStruxure Power Operation: - - 2024 CU1

Категория уязвимого продукта: Не определено

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.

14

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

Оценка CVSSv4: 6.9 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-03.pdf
- https://bdu.fstec.ru/vul/2023-06559

Краткое описание: Отказ в обслуживании в Schneider Electric EcoStruxure Power Operation

Идентификатор уязвимости: CVE-2023-35945
BDU:2025-04696

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

Уязвимый продукт: EcoStruxure Power Operation: - - 2024 CU1

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-03.pdf
- https://bdu.fstec.ru/vul/2025-04696

16

Краткое описание: Отказ в обслуживании в Schneider Electric EcoStruxure Power Operation

Идентификатор уязвимости: CVE-2022-45198
BDU:2023-02447

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

Уязвимый продукт: EcoStruxure Power Operation: - - 2024 CU1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-03.pdf
- https://bdu.fstec.ru/vul/2023-02447

Краткое описание: Выполнение произвольного кода в Schneider Electric EcoStruxure Power Operation

Идентификатор уязвимости: CVE-2023-50447
BDU:2024-00775

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

Уязвимый продукт: EcoStruxure Power Operation: - - 2024 CU1

Категория уязвимого продукта: Не определено

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.

17

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-03.pdf
- https://bdu.fstec.ru/vul/2024-00775

Краткое описание: Получение конфиденциальной информации в Schneider Electric EcoStruxure Power Operation

Идентификатор уязвимости: CVE-2022-22817
BDU:2022-00583

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

Уязвимый продукт: EcoStruxure Power Operation: - - 2024 CU1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

18

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-03.pdf
- https://bdu.fstec.ru/vul/2022-00583

Краткое описание: Обход безопасности в CrushFTP

Идентификатор уязвимости: CVE-2025-54309
BDU:2025-08775

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: CrushFTP: 10.0.0 - 11.3.3

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.

19

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-21 / 2025-07-21

Ссылки на источник:

- https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025#section-CompromiseJuly2025-CVE202554309
- https://www.bleepingcomputer.com/news/security/crushftp-zero-day-exploited-in-attacks-to-gain-admin-access-on-servers/
- https://www.rapid7.com/blog/post/crushftp-zero-day-exploited-in-the-wild/
- https://bdu.fstec.ru/vul/2025-08775

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2025-53770
BDU:2025-08714

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SharePoint Server: 2016 - 2019

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.

20

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-20 / 2025-07-20

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770
- https://bdu.fstec.ru/vul/2025-08714

21

Краткое описание: Выполнение произвольного кода в Autodesk Desktop products

Идентификатор уязвимости: CVE-2025-5039

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Infrastructure Parts Editor:
2026
Autodesk Inventor:
2026
Autodesk Navisworks Manage:
2026
Autodesk Navisworks Simulate:
2026
Revit:
2026
Autodesk Vault Basic Client:
2026

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-28 / 2025-07-28

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0014

22

Краткое описание: Выполнение произвольного кода в Leovo MediaTek WLAN driver

Идентификатор уязвимости: CVE-2024-20148

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) - ThinkBook 14 G6 ABP, ThinkBook 16 G6 ABP:
все версии
WLAN Driver (Mediatek, Realtek) for Windows 10 (64-bit) - ThinkBook 14 G6 ABP, ThinkBook 16 G6 ABP:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Yoga Pro 7 14APH8, Lenovo Slim Pro 7 14APH8:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion S5 14APH8:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion Pro 7 16ARX8H:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion 5 15ARP8:
все версии
WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) -IdeaPad Pro 5 16APH8:
все версии
MTK MT7921 WLAN Driver for Windows 10 (Version 20H2) - ThinkCentre M75q Gen 2 (Type 11JN, 11JQ, 11JR, 11JS):
все версии
Mediatek MT7921 Wireless LAN Driver for Windows 11 (Version 21H2 or later) and 10 (Version 20H2) - ThinkStation P350:
все версии
MTK WiFi Driver for Windows 11 (Version 21H2 or Later) - ThinkStation P348:
все версии
MTK WiFi Driver for Windows 10 (Version 21H2) - ThinkStation P348:
все версии
MediaTek MT7921 Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkStation P340:
все версии
MediaTek MT7921 Wireless LAN Driver for Windows 10 (Version 21H2) - ThinkStation P340:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Yoga Pro 7 14ASP9:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Yoga Pro 7 14AHP9:

все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Yoga 7 2-in-1 14AHP9, Yoga 7 2-in-1 16AHP9:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - ThinkBook 14 G7 ARP, ThinkBook 16 G7 ARP:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 10 (64-bit) - ThinkBook 14 G7 ARP, ThinkBook 16 G7 ARP:
все версии
Legion Go S 8ARP1:
все версии
Legion Go S 8APU1:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion 5 15APH9:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - IdeaPad Slim 5 14AHP10, IdeaPad Slim 5 16AHP10:
все версии
WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) - IdeaPad Pro 5 16AHP9:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - IdeaPad Pro 5 14AHP9:
все версии
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - IdeaPad 5 2-in-1 14AHP9, IdeaPad 5 2-in-1 16AHP9:
все версии
MediaTek WLAN Driver for Windows 11 64-bit (Version 21H2 or Later) - Yoga AIO 7 27APH8:
все версии
MediaTek Wireless LAN Driver for Windows 11 64-bit (Version 21H2 or Later) - Lenovo A100, Lenovo V100:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkCentre Neo 70t Gen 3:
все версии
MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre Neo 70t Gen 3:
все версии
MTK WLAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre Neo 30a 22 Gen 4, Neo 30a 24 Gen 4, Neo 30a 27 Gen 4:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkCentre M90s Gen 3, M90t Gen 3:
все версии

MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M90s Gen 3, M90t Gen 3:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkCentre M90q Gen 3:
все версии
MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M90q Gen 3:
все версии
MTK7921 Wireless LAN Driver for Windows 11 (Version 21H2 or Later), 10 (64-bit) - ThinkCentre M90a Pro Gen 3:
все версии
MediaTek RZ616 Wireless LAN Driver for Windows 11 (Version 21H2 or Later), 10 (64-bit) - ThinkCentre M90a Pro Gen 3:
все версии
MTK7921 Wireless LAN Driver for Windows 11 (Version 21H2 or Later), 10 (64-bit) - ThinkCentre M90a Gen 3:
все версии
MediaTek RZ616 Wireless LAN Driver for Windows 10 (64-bit), 11 (Version 21H2 or Later) - ThinkCentre M90a Gen 3:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkCentre M80s Gen 3, M80t Gen 3:
все версии
MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M80s Gen 3, M80t Gen 3:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkCentre M80q Gen 3:
все версии
MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M80q Gen 3:
все версии
Mediatek Wireless LAN Driver for Windows 10 (64-bit) IOT - Desktop, Workstation:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre M75t Gen 5:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre M75s Gen 5:
все версии
MTK Wireless LAN Driver for Windows 10 64-bit - ThinkCentre M75t Gen 5, M75s Gen 5:
все версии
MTK WLAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre M75t Gen 2, M75s Gen 2:
все версии
Mediatek Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M75t Gen 2, M75s Gen 2:

все версии
MTK WLAN Driver for Windows 10 (64-bit) - ThinkCentre M75t Gen 2, M75s Gen 2:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre M75t Gen 2, M75s Gen 2:
все версии
MTK Wireless LAN Driver for Windows 11 IOT (Version 24H2) - ThinkCentre M75s Gen 5, M75t Gen 5:
все версии
MTK Wireless LAN Driver for Windows 11 (Version 21H2 or Later) - ThinkCentre M75q Gen 5:
все версии
MTK Wireless LAN Driver for Windows 10 (64-bit) - ThinkCentre M75q Gen 5:
все версии
MTK7921 Wireless LAN Driver for Windows 10 (64-bit), 11 (Version 21H2 or later) - ThinkCentre M70a Gen 3:
все версии
MediaTek RZ616 Wireless LAN Driver for Windows 10 (64-bit), 11 (Version 21H2 or later) - ThinkCentre M70a Gen 3:
все версии
MTK MT7925 Wireless LAN Driver for Windows 11 64-bit (Version 21H2 or Later) - Legion T7 34IAS10:
все версии
Realtek Wireless LAN Driver for Windows 11 64-bit (Version 21H2 or Later) - IdeaCentre AIO 24ARR9, AIO 27ARR9:
все версии
MediaTek Wireless LAN Driver for Windows 11 64-bit (Version 21H2 or Later) - IdeaCentre AIO 24ARR9, AIO 27ARR9:
все версии
ThinkBook 16 G7+ ASP:
все версии
IdeaPad Slim 5 16AHP10:
все версии
IdeaPad Slim 5 15ARP10:
все версии
IdeaPad Slim 5 14AHP10:
все версии
IdeaPad Slim 5 13ARP10:
все версии
IdeaPad Slim 3 16AHP10:
все версии
IdeaPad Slim 3 15AHP10:

все версии
IdeaPad Slim 3 14AHP10:
все версии
Lenovo V15 G4 ABP:
все версии
Lenovo V14 G4 ABP:
все версии
Legion 5 15ARP8:
все версии
Yoga Pro 7 14ASP9:
все версии
Yoga Pro 7 14APH8:
все версии
Yoga Pro 7 14AHP9:
все версии
Yoga 7 2-in-1 16AHP9:
все версии
Yoga 7 2-in-1 14AHP9:
все версии
LOQ 16APH8:
все версии
LOQ 15ARP9:
все версии
LOQ 15APH8:
все версии
LOQ 15AHP9:
все версии
Lenovo Slim Pro 7 14APH8:
все версии
Legion Slim 5 16ARP9:
все версии
Legion Slim 5 16APH8:
все версии
Legion Slim 5 16AHP9:

все версии
Legion Slim 5 14APH8:
все версии
Legion S7 16APH8:
все версии
Legion Pro 7 16ARX8H:
все версии
Legion 5 15APH9:
все версии
IdeaPad Slim 5 16AHP9:
все версии
IdeaPad Slim 5 14AHP9:
все версии
IdeaCentre AIO 3 27ARR9:
все версии
IdeaCentre AIO 3 24ARR9:
все версии
ThinkCentre M75q Gen 5:
все версии
ThinkCentre M75t Gen 5:
все версии
ThinkCentre M75s Gen 5:
все версии
ThinkPad X13 Gen 3 21CN:
все версии
ThinkPad X13 Gen 3 21CM:
все версии
ThinkPad T14s Gen 3 21CR:
все версии
ThinkPad T14s Gen 3 21CQ:
все версии
ThinkPad E15 Gen 4 21EE:
все версии
ThinkPad E15 Gen 4 21ED:

все версии
ThinkPad E14 Gen 4 21EC:
все версии
ThinkPad E14 Gen 4 21EB:
все версии
ThinkBook 16 G7 ARP:
все версии
ThinkBook 14 G7 ARP:
все версии
IdeaPad Pro 5 16AHP9:
все версии
IdeaPad Pro 5 14AHP9:
все версии
IdeaPad 5 2-in-1 16AHP9:
все версии
IdeaPad 5 2-in-1 14AHP9:
все версии
WLAN Driver (Intel, Mediatek) for Windows 11 (64-bit) - Legion 9 16IRX9:
все версии
Legion T7 34IAS10:
все версии
ThinkBook 16 G6 ABP:
все версии
ThinkBook 14 G6 ABP:
все версии
Lenovo 13w Yoga Gen 2 82YS:
все версии
Lenovo 13w Yoga Gen 2 82YR:
все версии
Yoga AIO 7 27APH8:
все версии
ThinkCentre M75t Gen 2:
все версии
ThinkCentre M75t Gen 2 11RE:

все версии
ThinkCentre M75t Gen 2 11RD:
все версии
ThinkCentre M75t Gen 2 11RC:
все версии
ThinkCentre M75t Gen 2 11RB:
все версии
ThinkCentre M75s Gen 2:
все версии
ThinkCentre M75s Gen 2 11RA:
все версии
ThinkCentre M75s Gen 2 11R9:
все версии
ThinkCentre M75s Gen 2 11R8:
все версии
ThinkCentre M75s Gen 2 11R7:
все версии
ThinkCentre M75q Gen 2 11JS:
все версии
ThinkCentre M75q Gen 2 11JR:
все версии
ThinkCentre M75q Gen 2 11JQ:
все версии
ThinkCentre M75q Gen 2 11JN:
все версии
Lenovo V100:
все версии
Lenovo A100:
все версии
ThinkCentre Neo 30a 27 Gen 4:
все версии
ThinkCentre Neo 30a 24 Gen 4:
все версии
ThinkCentre Neo 30a 22 Gen 4:

все версии
IdeaPad Slim 3 16IRH10R:
все версии
IdeaPad Slim 3 16IRH10:
все версии
IdeaPad Slim 3 15IRU10:
все версии
IdeaPad Slim 3 15IRH10R:
все версии
IdeaPad Slim 3 15IRH10:
все версии
IdeaPad Slim 3 14IRU10:
все версии
IdeaPad Slim 3 14IRH10R:
все версии
IdeaPad Slim 3 14IRH10:
все версии
IdeaPad Pro 5 16APH8:
все версии
Legion 7 16IRX9:
все версии
ThinkStation P360 Workstation:
все версии
ThinkStation P350 Workstation:
все версии
ThinkStation P348 Workstation:
все версии
Legion 9 16IRX9:
все версии
ThinkCentre Neo 70t Gen 3:
все версии
ThinkCentre M90t Gen 3:
все версии
ThinkCentre M90s Gen 3:

все версии
ThinkCentre M90q Gen 3:
все версии
ThinkCentre M90a Gen 3 Pro:
все версии
ThinkCentre M90a Gen 3:
все версии
ThinkCentre M80t Gen 3:
все версии
ThinkCentre M80s Gen 3:
все версии
ThinkCentre M80q Gen 3:
все версии
ThinkCentre M70a Gen 3:
все версии
ThinkPad T16 Gen 1 21CJ:
все версии
ThinkPad T16 Gen 1 21CH:
все версии
ThinkPad T14 Gen 3 21CG:
все версии
ThinkPad T14 Gen 3 21CF:
все версии
ThinkPad P16s Gen 1 21CL:
все версии
ThinkPad P16s Gen 1 21CK:
все версии
ThinkPad P14s Gen 3 21J6:
все версии
ThinkPad P14s Gen 3 21J5:
все версии
ThinkPad Z16 Gen 1 21D5:
все версии
ThinkPad Z16 Gen 1 21D4:

все версии
ThinkPad Z13 Gen 1 21D3:
все версии
ThinkPad Z13 Gen 1 21D2:
все версии
ThinkStation P340 Workstation:
все версии
RZ616 Wireless LAN Driver for Windows 11 (Version 21H2 or later) - ThinkPad Z13 (Type 21D2, 21D3), Z16 (Type 21D4, 21D5):
до 25.40.2.579
Mediatek Wireless LAN Software for Windows 10 (Version 20H2 or later) - ThinkPad Z13 (Type 21D2, 21D3), Z16 (Type 21D4, 21D5):
до 25.40.2.579
RZ616 Wireless LAN Driver for Windows 11 (Version 21H2 or later), 10 (Version 20H2 or later) - ThinkPad:
до 25.40.2.579
RZ616 WLAN Driver for Windows 11 (Version 21H2 or later), 10 (Version 21H2 or later) - ThinkPad E14 Gen 4, E15 Gen 4:
до 25.40.2.579
Mediatek WLAN Driver for Windows 11 (64-bit) - ThinkBook 16 G7+ ASP:
до 25.20.3.47
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - LOQ 15ARP9:
до 25.40.2.579
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - LOQ 15APH8, LOQ 16APH8:
до 25.40.2.579
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - LOQ 15AHP9:
до 25.40.2.579
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Lenovo V14 G4 ABP, Lenovo V15 G4 ABP:
до 24.34.2.570
WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) - Legion Slim 5 16ARP9:
до 25.40.2.579
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion Slim 5 16APH8:
до 25.40.2.579
WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) - Legion Slim 5 16AHP9:
до 25.40.2.579

Mediatek WLAN Driver for Windows 11 (64-bit) - Legion S7 16APH8:
до 25.40.2.579
Mediatek WLAN Driver for Windows 11 (64-bit) - Legion Go S 8ARP1, Legion Go S 8APU1:
до 25.40.2.577
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - Legion 7 16IRX9:
до 25.20.3.47
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - IdeaPad Slim 5 14AHP9, IdeaPad Slim 5 16AHP9:
до 25.40.2.579
WLAN Driver (Mediatek, Realtek) for Windows 11 (64-bit) - IdeaPad Slim 5 13ARP10, IdeaPad Slim 5 15ARP10:
до 25.40.2.579
WLAN Driver (Realtek, Mediatek, Intel) for Windows 11 (64-bit) - IdeaPad Slim 3 14 15 16 Series:
до 24.20.3.37
WLAN Driver (Realtek, Mediatek) for Windows 11 (64-bit) - IdeaPad Slim 3 14AHP10,IdeaPad Slim 3 15AHP10,IdeaPad Slim 3 16AHP10:
до 24.20.3.37 & 24.10.5.4
Wireless Driver for Windows 11 (Version 22H2 or later) - Lenovo 13w Yoga Gen 2 (Type 82YR, 82YS):
до 25.40.2.579
Wireless Driver for Windows 10 64-bit (Version 22H2 or later) - Lenovo 13w Yoga Gen 2 (Type 82YR, 82YS):
до 25.40.2.579

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-28 / 2025-07-28

Ссылки на источник:

- https://support.lenovo.com/us/en/product_security/LEN-180830

23

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-8011

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

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 138.0.3351.95

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-28 / 2025-07-28

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-8011

24

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-8010

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

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 138.0.3351.95

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-28 / 2025-07-28

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-8010

Краткое описание: Отказ в обслуживании в Honeywell Experion PKS

Идентификатор уязвимости: CVE-2025-3947

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

Уязвимый продукт: Experion PKS:
до R520.2 TCU9 Hot Fix 1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

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.

25

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-25 / 2025-07-25

Ссылки на источник:

- https://process.honeywell.com/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS

Идентификатор уязвимости: CVE-2025-3946

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

Уязвимый продукт: Experion PKS:
до R520.2 TCU9 Hot Fix 1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-25 / 2025-07-25

Ссылки на источник:

- https://process.honeywell.com/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS

Идентификатор уязвимости: CVE-2025-2523

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

Уязвимый продукт: Experion PKS:
до R520.2 TCU9 Hot Fix 1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-25 / 2025-07-25

Ссылки на источник:

- https://process.honeywell.com/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS

Идентификатор уязвимости: CVE-2025-2521

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

Уязвимый продукт: Experion PKS:
до R520.2 TCU9 Hot Fix 1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-25 / 2025-07-25

Ссылки на источник:

- https://process.honeywell.com/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03

29

Краткое описание: Отказ в обслуживании в Honeywell Experion PKS

Идентификатор уязвимости: CVE-2025-2520
BDU:2025-08555

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: Experion PKS:
до R520.2 TCU9 Hot Fix 1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-25 / 2025-07-25

Ссылки на источник:

- https://process.honeywell.com/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03
- https://bdu.fstec.ru/vul/2025-08555

30

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2025-7656
BDU:2025-08887

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

Уязвимый продукт: Chrome OS:
до 136.0.7103.150

Категория уязвимого продукта: Не определено

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-24 / 2025-07-24

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/07/stable-chanel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2025-08887

31

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2025-6558
BDU:2025-08785

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Chrome OS:
до 136.0.7103.150

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-24 / 2025-07-24

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/07/stable-chanel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2025-08785

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2025-7657
BDU:2025-08879

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 136.0.7103.150

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

32

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-24 / 2025-07-24

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/07/stable-chanel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2025-08879

33

Краткое описание: Запись локальных файлов в SonicWall SMA100 SSL-VPN

Идентификатор уязвимости: CVE-2025-40599

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: SMA 100:
10.2.0.2-20sv - 10.2.1.15-81sv

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0014

34

Краткое описание: Выполнение произвольного кода в SonicWall SMA100 SSL-VPN

Идентификатор уязвимости: CVE-2025-40597

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

Уязвимый продукт: SMA 100:
10.2.0.2-20sv - 10.2.1.15-81sv

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0012

35

Краткое описание: Выполнение произвольного кода в Dahua products

Идентификатор уязвимости: CVE-2025-31701

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

Уязвимый продукт: IPC-1XXX Series:
все версии
IPC-2XXX Series:
все версии
IPC-WX Series:
все версии
IPC-ECXX Series:
все версии
SD3A Series:
все версии
SD2A Series:
все версии
SD3D Series:
все версии
SDT2A Series:
все версии
SD2C Series:
все версии

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.dahuasecurity.com/aboutUs/trustedCenter/details/775

36

Краткое описание: Выполнение произвольного кода в Dahua products

Идентификатор уязвимости: CVE-2025-31700

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

Уязвимый продукт: IPC-1XXX Series:
все версии
IPC-2XXX Series:
все версии
IPC-WX Series:
все версии
IPC-ECXX Series:
все версии
SD3A Series:
все версии
SD2A Series:
все версии
SD3D Series:
все версии
SDT2A Series:
все версии
SD2C Series:
все версии

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://www.dahuasecurity.com/aboutUs/trustedCenter/details/775

37

Краткое описание: Выполнение произвольного кода в Ruijie NBR

Идентификатор уязвимости: CVE-2025-34057
BDU:2025-08054

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

Уязвимый продукт: Ruijie серии NBR

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 0.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-02 / 2025-07-03

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-08054

38

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2025-25257
BDU:2025-08439

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

Уязвимый продукт: FortiWeb: 7.0.0 - 7.6.3

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-08 / 2025-07-08

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-151
- https://bdu.fstec.ru/vul/2025-08439

39

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-7656

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

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 138.0.3351.83

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-7656

40

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2025-6558

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 138.0.3351.83

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-6558

41

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-7657

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 138.0.3351.83

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-7657

42

Краткое описание: Выполнение произвольного кода в VMware products

Идентификатор уязвимости: CVE-2025-41238

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

Уязвимый продукт: VMware ESXi: ESXi70U1e-19324898 - ESXi80a-20842819
VMware Workstation: 17.0 - 17.6.3
VMware Fusion: 13.0 - 13.6.3
Cloud Foundation: before ESXi70U3w-24784741

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 2.5 AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/U:Green

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877

43

Краткое описание: Выполнение произвольного кода в VMware products

Идентификатор уязвимости: CVE-2025-41237
BDU:2025-08573

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

Уязвимый продукт: VMware ESXi: ESXi70U1e-19324898 - ESXi80a-20842819
VMware Workstation: 17.0 - 17.6.3
VMware Fusion: 13.0 - 13.6.3
Cloud Foundation: before ESXi70U3w-24784741

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 1.4 AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/U:Green

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877
- https://bdu.fstec.ru/vul/2025-08573

Краткое описание: Выполнение произвольного кода в VMware products

Идентификатор уязвимости: CVE-2025-41236
BDU:2025-08590

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

Уязвимый продукт: VMware ESXi: ESXi70U1e-19324898 - ESXi80a-20842819
VMware Workstation: 17.0 - 17.6.3
VMware Fusion: 13.0 - 13.6.3
Cloud Foundation: before ESXi70U3w-24784741

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

44

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-17 / 2025-07-17

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877
- https://bdu.fstec.ru/vul/2025-08590

Краткое описание: Выполнение произвольного кода в Oracle HTTP Server

Идентификатор уязвимости: CVE-2025-24928
BDU:2025-05193

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Oracle HTTP Server:
12.2.1.4.0 - 14.1.2.0.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

45

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:N/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?1389
- https://bdu.fstec.ru/vul/2025-05193

Краткое описание: Отказ в обслуживании в Oracle HTTP Server

Идентификатор уязвимости: CVE-2024-38477
BDU:2024-05195

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle HTTP Server:
12.2.1.4.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Отказ в обслуживании

46 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?1389
- https://bdu.fstec.ru/vul/2024-05195

47

Краткое описание: Выполнение произвольного кода в Oracle HTTP Server

Идентификатор уязвимости: CVE-2024-8176
BDU:2025-04573

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Oracle HTTP Server:
12.2.1.4.0 - 14.1.2.0.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?1389
- https://bdu.fstec.ru/vul/2025-04573

48

Краткое описание: Получение конфиденциальной информации в Oracle Java SE

Идентификатор уязвимости: CVE-2025-50059

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle GraalVM Enterprise Edition: 21.3.14

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?3082

49

Краткое описание: Выполнение произвольного кода в Oracle Java SE

Идентификатор уязвимости: CVE-2025-30749

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle GraalVM Enterprise Edition: 21.3.14

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?3082

50

Краткое описание: Выполнение произвольного кода в Oracle Java SE

Идентификатор уязвимости: CVE-2025-50106

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle GraalVM Enterprise Edition: 21.3.14

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?3082

Краткое описание: Выполнение произвольного кода в Oracle Java SE

Идентификатор уязвимости: CVE-2025-24855
BDU:2025-03640

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Oracle Java SE:
8u451 b50

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

51

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

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-16 / 2025-07-16

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpujul2025.html?3082
- https://bdu.fstec.ru/vul/2025-03640