НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-09-22.1 | 22 сентября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-8894	Autodesk products	Локальный	ACE	2025-09-19	✓
2	Высокая	CVE-2025-8893	Autodesk products	Локальный	ACE	2025-09-19	✓
3	Критическая	CVE-2025-0838	Abseil-cpp	Сетевой	ACE	2025-09-19	✓
4	Критическая	CVE-2025-8356	FUJIFILM Xerox Freeflow Core	Сетевой	WLF	2025-09-18	✓
5	Высокая	CVE-2025-8355	FUJIFILM Xerox Freeflow Core	Сетевой	OSI	2025-09-18	✓
6	Критическая	CVE-2025-58321	Delta Electronics DIALink	Сетевой	RLF	2025-09-17	✓
7	Высокая	CVE-2025-37125	HPE Aruba Networking EdgeConnect SD-WAN Gateways	Сетевой	OSI	2025-09-17	✓
8	Высокая	CVE-2025-37124	HPE Aruba Networking EdgeConnect SD-WAN Gateways	Сетевой	SB	2025-09-17	✓
9	Высокая	CVE-2025-37123	HPE Aruba Networking EdgeConnect SD-WAN Gateways	Сетевой	ACE	2025-09-17	✓
10	Высокая	CVE-2025-10535	Mozilla Firefox	Сетевой	OSI	2025-09-17	✓
11	Высокая	CVE-2025-10534	Mozilla Firefox	Сетевой	SUI	2025-09-17	✓
12	Высокая	CVE-2025-10537	Mozilla Firefox	Сетевой	ACE	2025-09-17	✓
13	Высокая	CVE-2025-10536	Mozilla Firefox	Локальный	OSI	2025-09-17	✓

14	Высокая	CVE-2025-10533	Mozilla Firefox	Сетевой	ACE	2025-09-17	✓
15	Высокая	CVE-2025-10123	D-Link DIR-823X	Сетевой	ACE	2025-09-17	✗
16	Критическая	CVE-2025-43359	macOS Sequoia	Сетевой	OSI	2025-09-16	✓
17	Критическая	CVE-2025-31255	macOS Sequoia	Сетевой	OSI	2025-09-16	✓
18	Высокая	CVE-2025-43330	macOS Sequoia	Локальный	PE	2025-09-16	✓
19	Высокая	CVE-2025-43298	macOS Sequoia	Локальный	PE	2025-09-16	✓
20	Высокая	CVE-2025-43286	macOS Sequoia	Локальный	PE	2025-09-16	✓
21	Высокая	CVE-2025-31259	macOS Sequoia	Локальный	PE	2025-09-16	✓
22	Критическая	CVE-2024-27280	macOS Sequoia	Сетевой	OSI	2025-09-16	✓
23	Высокая	CVE-2025-43358	macOS Sequoia	Локальный	PE	2025-09-16	✓
24	Высокая	CVE-2025-9807	The Events Calendar plugin for WordPress	Сетевой	ACE	2025-09-16	✓

1

Краткое описание: Выполнение произвольного кода в Autodesk products

Идентификатор уязвимости: CVE-2025-8894

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

Уязвимый продукт: Revit:
2025 - 2026.2
Autodesk AutoCAD:
2024 - 2026.0
AutoCAD Architecture:
2024 - 2026.0
AutoCAD Electrical:
2024 - 2026.0
AutoCAD Mechanical:
2024 - 2026.0
AutoCAD MEP:
2024 - 2026.0
AutoCAD Plant 3D:
2024 - 2026.0
AutoCAD Map 3D:
2024 - 2026.0
Autodesk Civil 3D:
2024 - 2026.0
Advance Steel:
2024 - 2026.0
AutoCAD LT:
2024 - 2026

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/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: 2025-09-19 / 2025-09-19

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0018

2

Краткое описание: Выполнение произвольного кода в Autodesk products

Идентификатор уязвимости: CVE-2025-8893
BDU:2025-11285

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Revit:
2025 - 2026.2
Autodesk AutoCAD:
2024 - 2026.0
AutoCAD Architecture:
2024 - 2026.0
AutoCAD Electrical:
2024 - 2026.0
AutoCAD Mechanical:
2024 - 2026.0
AutoCAD MEP:
2024 - 2026.0
AutoCAD Plant 3D:
2024 - 2026.0
AutoCAD Map 3D:
2024 - 2026.0
Autodesk Civil 3D:
2024 - 2026.0
Advance Steel:
2024 - 2026.0
AutoCAD LT:
2024 - 2026

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

Оценка CVSSv4: 5.7 AV:L/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: 2025-09-19 / 2025-09-19

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0018
- https://bdu.fstec.ru/vul/2025-11285

3

Краткое описание: Выполнение произвольного кода в Abseil-cpp

Идентификатор уязвимости: CVE-2025-0838
BDU:2025-10265

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

Уязвимый продукт: abseil-cpp:
20180600 - 20250814.0

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: 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: 2025-09-19 / 2025-09-19

Ссылки на источник:

- https://github.com/abseil/abseil-cpp/commit/5a0e2cb5e3958dd90bb8569a2766622cb74d90c1
- https://lists.debian.org/debian-lts-announce/2025/04/msg00012.html
- https://bdu.fstec.ru/vul/2025-10265

4

Краткое описание: Запись локальных файлов в FUJIFILM Xerox Freeflow Core

Идентификатор уязвимости: CVE-2025-8356

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

Уязвимый продукт: Xerox FreeFlow Core:
- - 8.0.4

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 9.8 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: 2025-09-18 / 2025-09-18

Ссылки на источник:

- https://securitydocs.business.xerox.com/wp-content/uploads/2025/08/Xerox-Security-Bulletin-025-013-for-Freeflow-Core-8.0.5.pdf
- https://horizon3.ai/attack-research/attack-blogs/from-support-ticket-to-zero-day/
- https://www.fujifilm.com/fbglobal/eng/company/news/notice/2025/0917_announce.html
- https://jvn.jp/en/vu/JVNVU90253343/index.html

5

Краткое описание: Получение конфиденциальной информации в FUJIFILM Xerox Freeflow Core

Идентификатор уязвимости: CVE-2025-8355

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Xerox FreeFlow Core:
- - 8.0.4

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 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:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-18 / 2025-09-18

Ссылки на источник:

- https://securitydocs.business.xerox.com/wp-content/uploads/2025/08/Xerox-Security-Bulletin-025-013-for-Freeflow-Core-8.0.5.pdf
- https://www.fujifilm.com/fbglobal/eng/company/news/notice/2025/0917_announce.html
- https://jvn.jp/en/vu/JVNVU90253343/index.html

6

Краткое описание: Чтение локальных файлов в Delta Electronics DIALink

Идентификатор уязвимости: CVE-2025-58321
BDU:2025-11017

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

Уязвимый продукт: DIALink:
- - 1.6.0.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/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: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2025-00016_DIALink%20-%20Directory%20Traversal%20Authentication%20Bypass%20Vulnerability.pdf
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-259-07
- https://bdu.fstec.ru/vul/2025-11017

7

Краткое описание: Получение конфиденциальной информации в HPE Aruba Networking EdgeConnect SD-WAN Gateways

Идентификатор уязвимости: CVE-2025-37125

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Aruba Networking EdgeConnect SD-WAN Gateways: до 9.4.3.5

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/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:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US

8

Краткое описание: Обход безопасности в HPE Aruba Networking EdgeConnect SD-WAN Gateways

Идентификатор уязвимости: CVE-2025-37124

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Aruba Networking EdgeConnect SD-WAN Gateways: до 9.2.11.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 6.8 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US

Краткое описание: Выполнение произвольного кода в HPE Aruba Networking EdgeConnect SD-WAN Gateways

Идентификатор уязвимости: CVE-2025-37123

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

Уязвимый продукт: Aruba Networking EdgeConnect SD-WAN Gateways:
- - 9.5.3.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-10535

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

Уязвимый продукт: Firefox for Android:
140.0 - 142.0.1

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.

10

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-73/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1979918

Краткое описание: Пользовательский интерфейс подмены в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-10534

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

Уязвимый продукт: Mozilla Firefox:
140.0 - 142.0.1
Firefox for Android:
140.0 - 142.0.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Пользовательский интерфейс подмены

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: 8.1 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:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-73/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1665334

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-10537

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

Уязвимый продукт: Mozilla Firefox:
128.0 - 142.0.1
Firefox ESR:
128.0 - 140.2.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2025-73/
- https://www.mozilla.org/security/advisories/mfsa2025-75/

13

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-10536

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

Уязвимый продукт: Mozilla Firefox:
128.0 - 142.0.1
Firefox ESR:
128.0 - 140.2.0

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://bugzilla.mozilla.org/show_bug.cgi?id=1981502
- https://www.mozilla.org/security/advisories/mfsa2025-73/
- https://www.mozilla.org/security/advisories/mfsa2025-75/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-10533

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

Уязвимый продукт: Mozilla Firefox:
128.0 - 142.0.1
Firefox ESR:
115.0 - 140.2.0
Firefox for Android:
110.0 - 142.0.1

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://bugzilla.mozilla.org/show_bug.cgi?id=1980788
- https://www.mozilla.org/security/advisories/mfsa2025-73/
- https://www.mozilla.org/security/advisories/mfsa2025-74/
- https://www.mozilla.org/security/advisories/mfsa2025-75/

Краткое описание: Выполнение произвольного кода в D-Link DIR-823X

Идентификатор уязвимости: CVE-2025-10123

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

Уязвимый продукт: DIR-823X:
- - 250416

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

15

Оценка CVSSv3: 7.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

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: 2025-09-17 / 2025-09-17

Ссылки на источник:

- https://github.com/lin-3-start/lin-cve/blob/main/DIR-823X/D-Link%20DIR-823X%20routers%20have%20an%20unauthorized%20command%20execution%20vulnerability.md
- https://github.com/lin-3-start/lin-cve/blob/main/DIR-823X/D-Link%20DIR-823X%20routers%20have%20an%20unauthorized%20command%20execution%20vulnerability.md#poc
- https://vuldb.com/?ctiid.323093
- https://vuldb.com/?id.323093
- https://vuldb.com/?submit.645712
- https://www.dlink.com/

16

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43359

Идентификатор программной ошибки: CWE-371 Уязвимости, связанные с состоянием

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 1.7 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

17

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-31255
BDU:2025-11289

Идентификатор программной ошибки: CWE-371 Уязвимости, связанные с состоянием

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 1.1 AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111
- https://bdu.fstec.ru/vul/2025-11289

18

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43330

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных 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:N/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

19

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43298

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43286

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

20 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

21

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-31259

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2024-27280
BDU:2024-02456

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Получение конфиденциальной информации

22

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 6.6 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:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111
- https://bdu.fstec.ru/vul/2024-02456

23

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43358

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: macOS:
15.0 24A335 - 15.6.1 24G90

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 1.1 AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://support.apple.com/en-us/125111

Краткое описание: Выполнение произвольного кода в The Events Calendar plugin for WordPress

Идентификатор уязвимости: CVE-2025-9807

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

Уязвимый продукт: The Events Calendar:
6.15.0 - 6.15.0.1

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.

24

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-16 / 2025-09-16

Ссылки на источник:

- https://plugins.trac.wordpress.org/browser/the-events-calendar/tags/6.15.0.1/src/Events/Custom_Tables/V1/WP_Query/Custom_Tables_Query.php#L682
- https://www.wordfence.com/threat-intel/vulnerabilities/id/8ea2ce90-6c8c-4a31-8faa-4ab99879d8b8?source=cve