НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-11-12.1 | 12 ноября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-43372	Apple macOS Sonoma	Локальный	PE	2025-11-04	✓
2	Высокая	CVE-2025-43474	Apple macOS Sonoma	Локальный	DoS	2025-11-04	✓
3	Высокая	CVE-2025-43401	Apple macOS Sonoma	Сетевой	DoS	2025-11-04	✓
4	Высокая	CVE-2025-43472	Apple macOS Sonoma	Локальный	ACE	2025-11-04	✓
5	Высокая	CVE-2025-43361	Apple macOS Sonoma	Локальный	OSI	2025-11-04	✓
6	Высокая	CVE-2025-43407	Apple macOS Sonoma	Локальный	SB	2025-11-04	✓
7	Высокая	CVE-2025-43373	Apple macOS Sonoma	Сетевой	PE	2025-11-04	✓
8	Высокая	CVE-2025-43413	Apple macOS Sonoma	Сетевой	PE	2025-11-04	✓
9	Высокая	CVE-2025-43476	Apple macOS Sonoma	Локальный	PE	2025-11-04	✓
10	Высокая	CVE-2024-49761	Apple macOS Sonoma	Сетевой	DoS	2025-11-04	✓
11	Высокая	CVE-2025-43405	Apple macOS Sonoma	Сетевой	OSI	2025-11-04	✓
12	Критическая	CVE-2025-30465	Apple macOS Sonoma	Сетевой	OSI	2025-11-04	✓
13	Высокая	CVE-2025-43361	macOS Sequoia	Локальный	OSI	2025-11-04	✓

14	Высокая	CVE-2025-43474	macOS Sequoia	Локальный	DoS	2025-11-04	✓
15	Высокая	CVE-2025-43387	macOS Sequoia	Локальный	PE	2025-11-04	✓
16	Высокая	CVE-2025-43401	macOS Sequoia	Сетевой	DoS	2025-11-04	✓
17	Высокая	CVE-2025-43472	macOS Sequoia	Локальный	ACE	2025-11-04	✓
18	Высокая	CVE-2025-43407	macOS Sequoia	Локальный	SB	2025-11-04	✓
19	Высокая	CVE-2025-43413	macOS Sequoia	Сетевой	PE	2025-11-04	✓
20	Высокая	CVE-2025-43373	macOS Sequoia	Сетевой	PE	2025-11-04	✓
21	Высокая	CVE-2025-43399	macOS Sequoia	Сетевой	OSI	2025-11-04	✓
22	Высокая	CVE-2025-43496	macOS Sequoia	Сетевой	OSI	2025-11-04	✓
23	Критическая	CVE-2025-30465	macOS Sequoia	Сетевой	OSI	2025-11-04	✓
24	Высокая	CVE-2024-49761	macOS Sequoia	Сетевой	DoS	2025-11-04	✓
25	Высокая	CVE-2025-43405	macOS Sequoia	Сетевой	OSI	2025-11-04	✓
26	Высокая	CVE-2025-43476	macOS Sequoia	Локальный	PE	2025-11-04	✓
27	Высокая	CVE-2025-43387	Apple macOS Tahoe	Локальный	PE	2025-11-04	✓
28	Высокая	CVE-2025-43474	Apple macOS Tahoe	Локальный	DoS	2025-11-04	✓

29	Высокая	CVE-2025-43496	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
30	Высокая	CVE-2025-43364	Apple macOS Tahoe	Локальный	PE	2025-11-04	✓
31	Высокая	CVE-2025-43413	Apple macOS Tahoe	Сетевой	PE	2025-11-04	✓
32	Высокая	CVE-2025-43462	Apple macOS Tahoe	Сетевой	PE	2025-11-04	✓
33	Высокая	CVE-2025-43436	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
34	Высокая	CVE-2025-43401	Apple macOS Tahoe	Сетевой	DoS	2025-11-04	✓
35	Высокая	CVE-2025-43407	Apple macOS Tahoe	Локальный	SB	2025-11-04	✓
36	Высокая	CVE-2025-43405	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
37	Высокая	CVE-2025-43480	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
38	Высокая	CVE-2025-43433	Apple macOS Tahoe	Сетевой	ACE	2025-11-04	✓
39	Высокая	CVE-2025-43431	Apple macOS Tahoe	Сетевой	ACE	2025-11-04	✓
40	Высокая	CVE-2025-43472	Apple macOS Tahoe	Локальный	ACE	2025-11-04	✓
41	Высокая	CVE-2024-49761	Apple macOS Tahoe	Сетевой	DoS	2025-11-04	✓
42	Высокая	CVE-2025-43502	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
43	Высокая	CVE-2025-43500	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓

44	Высокая	CVE-2025-43476	Apple macOS Tahoe	Локальный	PE	2025-11-04	✓
45	Высокая	CVE-2025-43399	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
46	Критическая	CVE-2025-30465	Apple macOS Tahoe	Сетевой	OSI	2025-11-04	✓
47	Высокая	CVE-2025-43502	Apple Safari	Сетевой	OSI	2025-11-04	✓
48	Высокая	CVE-2025-43480	Apple Safari	Сетевой	OSI	2025-11-04	✓
49	Высокая	CVE-2025-43433	Apple Safari	Сетевой	ACE	2025-11-04	✓
50	Высокая	CVE-2025-43431	Apple Safari	Сетевой	ACE	2025-11-04	✓
51	Высокая	CVE-2025-43431	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2025-11-04	✓
52	Высокая	CVE-2025-43433	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2025-11-04	✓
53	Высокая	CVE-2025-43480	WebKitGTK+ and WPE WebKit	Сетевой	OSI	2025-11-04	✓
54	Высокая	CVE-2025-12430	Google Chrome и Microsoft Edge	Сетевой	ACE	2025-10-30	✓
55	Высокая	CVE-2025-12432	Google Chrome и Microsoft Edge	Сетевой	ACE	2025-10-30	✓
56	Высокая	CVE-2025-12436	Google Chrome и Microsoft Edge	Сетевой	ACE	2025-10-30	✓
57	Высокая	CVE-2025-12437	Google Chrome и Microsoft Edge	Сетевой	OSI	2025-10-30	✓
58	Высокая	CVE-2025-12428	Google Chrome и Microsoft Edge	Сетевой	ACE	2025-10-30	✓

59	Высокая	CVE-2025-12438	Google Chrome и Microsoft Edge	Сетевой	OSI	2025-10-30	✓
60	Высокая	CVE-2025-62579	Delta Electronics ASDA-Soft	Локальный	ACE	2025-10-30	✓
61	Высокая	CVE-2025-62580	Delta Electronics ASDA-Soft	Локальный	ACE	2025-10-30	✓
62	Высокая	CVE-2025-10934	GIMP	Локальный	ACE	2025-10-30	✓
63	Высокая	CVE-2025-60751	GeographicLib	Сетевой	ACE	2025-10-29	✓
64	Критическая	CVE-2025-12380	Mozilla Firefox	Сетевой	ACE	2025-10-29	✓
65	Высокая	CVE-2025-58317	Delta Electronics CNCSoft-G2	Локальный	ACE	2025-10-29	✓
66	Высокая	CVE-2025-58319	Delta Electronics CNCSoft-G2	Локальный	ACE	2025-10-29	✓

1

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43372

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

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:N/UI:R/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: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

2

Краткое описание: Отказ в обслуживании в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43474

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 4.3 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

3

Краткое описание: Отказ в обслуживании в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43401

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем 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: 1.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

4

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43472

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR: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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

5

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43361

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Чтение за пределами буфера.

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: 7.8 AV:L/AC:L/PR:L/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: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

6

Краткое описание: Обход безопасности в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43407

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 7.8 AV:L/AC:L/PR:N/UI:R/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:L/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

7

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43373

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

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

8

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43413

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

9

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43476

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

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

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: 7.8 AV:L/AC:L/PR:N/UI:R/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: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

10

Краткое описание: Отказ в обслуживании в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-49761
BDU:2024-09876

Идентификатор программной ошибки: CWE-1333 Неэффективные из-за своей сложности регулярные выражения

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636
- https://bdu.fstec.ru/vul/2024-09876

11

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-43405

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

12

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2025-30465

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

Уязвимый продукт: macOS:
14.0 23A344 - 14.8.1 23J30

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125636

13

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43361

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Чтение за пределами буфера.

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: 7.8 AV:L/AC:L/PR:L/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: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

14

Краткое описание: Отказ в обслуживании в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43474

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 4.3 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

15

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43387

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

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: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

16

Краткое описание: Отказ в обслуживании в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43401

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем 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: 1.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

17

Краткое описание: Выполнение произвольного кода в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43472

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR: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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

18

Краткое описание: Обход безопасности в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43407

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 7.8 AV:L/AC:L/PR:N/UI:R/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:L/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

19

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43413

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

20

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43373

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

21

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43399

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Непреднамеренное предоставление чувствительной информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

22

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43496

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/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:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

23

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-30465

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

Краткое описание: Отказ в обслуживании в macOS Sequoia

Идентификатор уязвимости: CVE-2024-49761
BDU:2024-09876

Идентификатор программной ошибки: CWE-1333 Неэффективные из-за своей сложности регулярные выражения

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

24

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635
- https://bdu.fstec.ru/vul/2024-09876

25

Краткое описание: Получение конфиденциальной информации в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43405

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

26

Краткое описание: Повышение привилегий в macOS Sequoia

Идентификатор уязвимости: CVE-2025-43476

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

Уязвимый продукт: macOS:
15.0 24A335 - 15.7.1 24G231

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: 7.8 AV:L/AC:L/PR:N/UI:R/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: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125635

27

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43387

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

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: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

28

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43474

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 4.3 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

29

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43496

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/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:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43364

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/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: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

31

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43413

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43462

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

33

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43436

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

34

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43401

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем 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: 1.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

35

Краткое описание: Обход безопасности в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43407

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 7.8 AV:L/AC:L/PR:N/UI:R/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:L/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

36

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43405

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

37

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43480

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple 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: 8.1 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:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

38

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43433

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

39

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43431

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

40

Краткое описание: Выполнение произвольного кода в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43472

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR: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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

41

Краткое описание: Отказ в обслуживании в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2024-49761
BDU:2024-09876

Идентификатор программной ошибки: CWE-1333 Неэффективные из-за своей сложности регулярные выражения

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634
- https://bdu.fstec.ru/vul/2024-09876

42

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43502

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

43

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43500

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

44

Краткое описание: Повышение привилегий в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43476

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

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: 7.8 AV:L/AC:L/PR:N/UI:R/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: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

45

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-43399

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Непреднамеренное предоставление чувствительной информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

Краткое описание: Получение конфиденциальной информации в Apple macOS Tahoe

Идентификатор уязвимости: CVE-2025-30465

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

Уязвимый продукт: macOS:
26.0 RC - 26.0.1 25A8364

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

47

Краткое описание: Получение конфиденциальной информации в Apple Safari

Идентификатор уязвимости: CVE-2025-43502

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Apple Safari:
17.0 - 26.0

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125640

48

Краткое описание: Получение конфиденциальной информации в Apple Safari

Идентификатор уязвимости: CVE-2025-43480

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Apple Safari:
17.0 - 26.0

Категория уязвимого продукта: Операционные системы Apple 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: 8.1 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:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125640

Краткое описание: Выполнение произвольного кода в Apple Safari

Идентификатор уязвимости: CVE-2025-43433

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

Уязвимый продукт: Apple Safari:
17.0 - 26.0

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

49

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125640

50

Краткое описание: Выполнение произвольного кода в Apple Safari

Идентификатор уязвимости: CVE-2025-43431

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

Уязвимый продукт: Apple Safari:
17.0 - 26.0

Категория уязвимого продукта: Операционные системы Apple 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125640

Краткое описание: Выполнение произвольного кода в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2025-43431

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

Уязвимый продукт: WebKitGTK+:
все версии
WPE WebKit:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

51

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR: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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

Краткое описание: Выполнение произвольного кода в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2025-43433

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

Уязвимый продукт: WebKitGTK+:
все версии
WPE WebKit:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

52

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

Краткое описание: Получение конфиденциальной информации в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2025-43480

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: WebKitGTK+:
все версии
WPE WebKit:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

53

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-04 / 2025-11-04

Ссылки на источник:

- https://support.apple.com/en-us/125634

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

Идентификатор уязвимости: CVE-2025-12430

Идентификатор программной ошибки: CWE-664 Некорректное обращение с ресурсом на протяжении его жизненного цикла

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

54

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2.7 AV:N/AC:L/AT:N/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: Требуется

Дата выявления / Дата обновления: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/442860743
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12430

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

Идентификатор уязвимости: CVE-2025-12432

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

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.5 AV:N/AC:H/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: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/439522866
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12432

56

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

Идентификатор уязвимости: CVE-2025-12436

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/40054742
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12436

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2025-12437

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Получение конфиденциальной информации

57 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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:N/A:H

Оценка CVSSv4: 4.6 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/446294487
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12437

58

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

Идентификатор уязвимости: CVE-2025-12428

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

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/447613211
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12428

59

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2025-12438

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.52
Microsoft Edge:
100.0.1185.29 - 141.0.3537.99

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: 4.6 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://crbug.com/433027577
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-12438

Краткое описание: Выполнение произвольного кода в Delta Electronics ASDA-Soft

Идентификатор уязвимости: CVE-2025-62579

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: ASDA-Soft:
- - 7.0.2.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

60

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: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-977/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-296-04

61

Краткое описание: Выполнение произвольного кода в Delta Electronics ASDA-Soft

Идентификатор уязвимости: CVE-2025-62580

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: ASDA-Soft:
- - 7.0.2.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-976/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-296-04

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2025-10934

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

Уязвимый продукт: Gimp:
3.0.0 - 3.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

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.

62

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: 2025-10-30 / 2025-10-30

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-978/
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14814

Краткое описание: Выполнение произвольного кода в GeographicLib

Идентификатор уязвимости: CVE-2025-60751

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: geographiclib:
1.0 - 2.5.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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.

63

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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: 2025-10-29 / 2025-10-29

Ссылки на источник:

- https://github.com/geographiclib/geographiclib/issues/43
- https://github.com/zer0matt/CVE-2025-60751

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-12380

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
142.0 - 144.0
Firefox for Android:
142.0 - 144.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

64 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2025-10-29 / 2025-10-29

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-86/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1993113

65

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2025-58317

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-G2:
- - 2.1.0.27

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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: 2025-10-29 / 2025-10-29

Ссылки на источник:

- https://www.deltaww.com/en-US/Cybersecurity_Advisory

66

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2025-58319

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-G2:
- - 2.1.0.27

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-10-29 / 2025-10-29

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-967/