НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-12-08.1 | 8 декабря 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2025-55182	React	Сетевой	ACE	2025-12-03	✓
2	Высокая	CVE-2025-66476	Vim for Windows	Локальный	OSI	2025-12-03	✓
3	Высокая	CVE-2025-13639	Google Chrome	Сетевой	OSI	2025-12-02	✓
4	Высокая	CVE-2025-13638	Google Chrome	Сетевой	DoS	2025-12-02	✓
5	Высокая	CVE-2025-13721	Google Chrome	Сетевой	SB	2025-12-02	✓
6	Высокая	CVE-2025-13720	Google Chrome	Сетевой	OSI	2025-12-02	✓
7	Высокая	CVE-2025-13633	Google Chrome	Сетевой	ACE	2025-12-02	✓
8	Средняя	CVE-2025-13632	Google Chrome	Сетевой	OSI	2025-12-02	✓
9	Высокая	CVE-2025-13631	Google Chrome	Сетевой	OSI	2025-12-02	✓
10	Высокая	CVE-2025-13630	Google Chrome	Сетевой	ACE	2025-12-02	✓
11	Высокая	CVE-2025-13699	MariaDB	Локальный	WLF	2025-12-01	✓
12	Высокая	CVE-2025-44018	GL-Inet GL-AXT1800	Сетевой	OSI	2025-11-25	✓
13	Высокая	CVE-2025-13552	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗

14	Высокая	CVE-2025-13551	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗
15	Высокая	CVE-2025-13550	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗
16	Высокая	CVE-2025-13549	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗
17	Высокая	CVE-2025-13548	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗
18	Высокая	CVE-2025-13547	D-Link DIR-822K, DWR-M920	Сетевой	ACE	2025-11-25	✗
19	Критическая	CVE-2025-64446	FortiWeb	Сетевой	ACE	2025-11-14	✓
20	Высокая	CVE-2025-20343	Cisco Identity Services Engine (ISE)	Сетевой	DoS	2025-11-05	✓
21	Высокая	CVE-2025-20341	Cisco Catalyst Center Virtual Appliance	Сетевой	PE	2025-11-13	✓
22	Критическая	CVE-2025-20358	Cisco Unified Contact Center Express	Сетевой	ACE	2025-11-05	✓
23	Критическая	CVE-2025-20354	Cisco Unified Contact Center Express	Сетевой	ACE	2025-11-05	✓
24	Высокая	CVE-2025-58034	FortiWeb	Сетевой	ACE	2025-11-18	✓

1

Краткое описание: Выполнение произвольного кода в React

Идентификатор уязвимости: CVE-2025-55182

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: React:
19.0.0 - 19.2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-03 / 2025-12-03

Ссылки на источник:

- https://www.facebook.com/security/advisories/cve-2025-55182
- https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

2

Краткое описание: Получение конфиденциальной информации в Vim for Windows

Идентификатор уязвимости: CVE-2025-66476

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Vim:
9.1.0 - 9.1.1946

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2025-12-03 / 2025-12-03

Ссылки на источник:

- https://github.com/vim/vim/security/advisories/GHSA-g77q-xrww-p834

3

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-13639

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

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: 0.5 AV:N/AC:L/AT:P/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: Требуется

Дата выявления / Дата обновления: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/448408148

4

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2025-13638

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 0.5 AV:N/AC:L/AT:P/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: Требуется

Дата выявления / Дата обновления: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/448046109

5

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2025-13721

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 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 7.5 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: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/355120682

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-13720

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/457818670

7

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-13633

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

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: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/458082926

8

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-13632

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/439058242

9

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-13631

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/448113221

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-13630

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

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 142.0.7444.177

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.

10

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-02 / 2025-12-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://crbug.com/456547591

11

Краткое описание: Запись локальных файлов в MariaDB

Идентификатор уязвимости: CVE-2025-13699

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

Уязвимый продукт: MariaDB:
10.6.0 - 11.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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

Оценка CVSSv4: 4.0 AV:L/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-01 / 2025-12-01

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1025/
- https://jira.mariadb.org/browse/MDEV-37483

12

Краткое описание: Получение конфиденциальной информации в GL-Inet GL-AXT1800

Идентификатор уязвимости: CVE-2025-44018

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: GL-AXT1800:
4.7.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка сертификатов.

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2230

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13552
BDU:2025-14606

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

Уязвимый продукт: DIR-822K:
1.00_20250513164613 - 1.1.50
DWR-M920:
1.00_20250513164613 - 1.1.50

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

13

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14606

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13551
BDU:2025-14751

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

Уязвимый продукт: DIR-822K:
1.00_20250513164613 - 1.1.50
DWR-M920:
1.00_20250513164613 - 1.1.50

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

14

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14751

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13550
BDU:2025-14753

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

Уязвимый продукт: DIR-822K:
1.00_20250513164613 - 1.1.50
DWR-M920:
1.00_20250513164613 - 1.1.50

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

15

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14753

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13549
BDU:2025-14754

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

Уязвимый продукт: DIR-822K:
1.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14754

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13548
BDU:2025-14752

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

Уязвимый продукт: DIR-822K:
1.00_20250513164613 - 1.1.50
DWR-M920:
1.00_20250513164613 - 1.1.50

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

17

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14752

Краткое описание: Выполнение произвольного кода в D-Link DIR-822K, DWR-M920

Идентификатор уязвимости: CVE-2025-13547
BDU:2025-14750

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

Уязвимый продукт: DIR-822K:
1.00_20250513164613 - 1.1.50
DWR-M920:
1.00_20250513164613 - 1.1.50

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

18

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.4 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-25 / 2025-11-25

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10476
- https://bdu.fstec.ru/vul/2025-14750

19

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2025-64446

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

Уязвимый продукт: FortiWeb:
7.0.0 - 8.0.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-14 / 2025-11-14

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-910

Краткое описание: Отказ в обслуживании в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2025-20343

Идентификатор программной ошибки: CWE-697 Некорректное сравнение

Уязвимый продукт: Cisco Identity Services Engine (ISE):
3.4 - 3.4P1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

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

20

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

Оценка CVSSv4: 4.9 AV:A/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: 2025-11-05 / 2025-11-05

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsupress-dos-8YF3JThh
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq27605

Краткое описание: Повышение привилегий в Cisco Catalyst Center Virtual Appliance

Идентификатор уязвимости: CVE-2025-20341

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco Catalyst Center Virtual Appliance:
2.3.7.4-VA - 2.3.7.9-VA

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 6.2 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-13 / 2025-11-13

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catc-priv-esc-VS8EeCuX
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo97875

Краткое описание: Выполнение произвольного кода в Cisco Unified Contact Center Express

Идентификатор уязвимости: CVE-2025-20358

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

Уязвимый продукт: Cisco Unified Contact Center Express:
до 12.5 SU3 ES07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

22

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

Оценка CVSSv4: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:U/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-05 / 2025-11-05

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq36573

Краткое описание: Выполнение произвольного кода в Cisco Unified Contact Center Express

Идентификатор уязвимости: CVE-2025-20354

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

Уязвимый продукт: Cisco Unified Contact Center Express:
до 12.5 SU3 ES07

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

23

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:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-05 / 2025-11-05

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq36528

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2025-58034

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

Уязвимый продукт: FortiWeb:
7.0.0 - 8.0.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv4: 8.6 AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-18 / 2025-11-18

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-513
- https://www.zerodayinitiative.com/advisories/ZDI-25-1014/