

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

## Бюллетень об уязвимостях программного обеспечения

VULN.2024-11-11.1 | 11 ноября 2024 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-20536	Cisco Nexus Dashboard Fabric Controller	Сетевой	ACE	2024-11-07	✓
2	Высокая	CVE-2024-20484	Cisco Enterprise Chat и Email	Сетевой	DoS	2024-11-07	✓
3	Высокая	CVE-2024-8746	File Manager Pro plugin for WordPress	Сетевой	ACE	2024-11-08	✓
4	Высокая	CVE-2024-8507	File Manager Pro plugin for WordPress	Сетевой	XSS\CSS	2024-11-08	✓
5	Высокая	CVE-2024-39354	Delta Electronics DIAScreen	Локальный	ACE	2024-11-08	✓
6	Высокая	CVE-2024-39605	Delta Electronics DIAScreen	Локальный	ACE	2024-11-08	✓
7	Высокая	CVE-2024-47131	Delta Electronics DIAScreen	Локальный	ACE	2024-11-08	✓
8	Критическая	CVE-2024-47460	ArubaOS и InstantOS	Сетевой	ACE	2024-11-06	✓
9	Критическая	CVE-2024-42509	ArubaOS и InstantOS	Сетевой	ACE	2024-11-06	✓
10	Критическая	CVE-2024-40638	GLPI	Сетевой	ACE	2024-11-06	✓
11	Критическая	CVE-2024-47758	GLPI	Сетевой	OSI	2024-11-06	✓
12	Критическая	CVE-2024-47761	GLPI	Сетевой	SB	2024-11-06	✓
13	Критическая	CVE-2024-47760	GLPI	Сетевой	OSI	2024-11-06	✓

14	Критическая	CVE-2024-50339	GLPI	Сетевой	ACE	2024-11-06	✓
15	Высокая	CVE-2022-36943	ZipArchive	Сетевой	OAF	2024-11-06	✓
16	Критическая	CVE-2024-51504	Apache ZooKeeper	Сетевой	ACE	2024-11-06	✓
17	Критическая	CVE-2024-20418	Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Points	Сетевой	ACE	2024-11-07	✓
18	Высокая	CVE-2024-10827	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-11-07	✓
19	Высокая	CVE-2024-10826	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-11-07	✓
20	Критическая	CVE-2024-20412	Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100 and 4200 Series	Локальный	OSI	2024-10-25	✓
21	Критическая	CVE-2024-20329	Cisco Adaptive Security Appliance Software	Сетевой	ACE	2024-10-25	✓

**Краткое описание:** Выполнение произвольного кода в Cisco Nexus Dashboard Fabric Controller

**Идентификатор уязвимости:** CVE-2024-20536  
BDU:2024-09233

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

**Уязвимый продукт:** Cisco Nexus Dashboard Fabric Controller (NDFC): с версии 12.1.2 по 12.1.3

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально созданных запросов.

**Последствия эксплуатации:** Выполнение произвольного кода

1

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-07 / 2024-11-07

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxl>
- <https://bdu.fstec.ru/vul/2024-09233>

**Краткое описание:** Отказ в обслуживании в Cisco Enterprise Chat и Email

**Идентификатор уязвимости:** CVE-2024-20484

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Enterprise Chat and Email: с версии 12.5 по 12.6

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

2

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-07 / 2024-11-07

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv>

**Краткое описание:** Выполнение произвольного кода в File Manager Pro plugin for WordPress

**Идентификатор уязвимости:** CVE-2024-8746

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

**Уязвимый продукт:** File Manager Pro: 8.3.9

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Выполнение 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:** 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-08 / 2024-11-08

**Ссылки на источник:**

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/88f1eb9a-f3bb-4b62-975f-a6cb95850966?source=cve>
- <http://filemanagerpro.io/>

**Краткое описание:** Межсайтовый скриптинг в File Manager Pro plugin for WordPress

**Идентификатор уязвимости:** CVE-2024-8507

**Идентификатор программной ошибки:** CWE-352 Подделка межсайтового запроса (CSRF)

**Уязвимый продукт:** File Manager Pro: 8.3.9

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Межсайтовый скриптинг

4

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-08 / 2024-11-08

**Ссылки на источник:**

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/db70b37c-707a-47b8-a3a2-5a2b7d30de89?source=cve>
- <http://filemanagerpro.io/>

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAScreen

Идентификатор уязвимости: CVE-2024-39354

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DIAScreen: до версии 1.5.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-08 / 2024-11-08

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1470/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1464/>

**Краткое описание:** Выполнение произвольного кода в Delta Electronics DIAScreen

**Идентификатор уязвимости:** CVE-2024-39605

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** DIAScreen: до версии 1.5.0

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**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:N/I:H/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-08 / 2024-11-08

**Ссылки на источник:**

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1469/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1467/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1465/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1462/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1461/>

**Краткое описание:** Выполнение произвольного кода в Delta Electronics DIAScreen

**Идентификатор уязвимости:** CVE-2024-47131

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** DIAScreen: до версии 1.5.0

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-08 / 2024-11-08

**Ссылки на источник:**

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1468/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1466/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1463/>

**Краткое описание:** Выполнение произвольного кода в ArubaOS и InstantOS

**Идентификатор уязвимости:** CVE-2024-47460

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

**Уязвимый продукт:** ArubaOS и InstantOS:  
ArubaOS: с версии 10.3.0.0 по 10.6.0.3  
Aruba InstantOS: с версии 8.10.0.13 по 8.12.0.2

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

**Способ эксплуатации:** Отправка специально сформированных данных.

8 **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:** 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- [http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en\\_us&docLocale=en\\_US](http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US)

**Краткое описание:** Выполнение произвольного кода в ArubaOS и InstantOS

**Идентификатор уязвимости:** CVE-2024-42509

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

**Уязвимый продукт:** ArubaOS и InstantOS:  
ArubaOS: с версии 10.3.0.0 по 10.6.0.3  
Aruba InstantOS: с версии 8.10.0.13 по 8.12.0.2

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

**Способ эксплуатации:** Отправка специально сформированных данных.

9 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- [http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en\\_us&docLocale=en\\_US](http://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US)

**Краткое описание:** Выполнение произвольного кода в GLPI

**Идентификатор уязвимости:** CVE-2024-40638

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

**Уязвимый продукт:** GLPI: с версии 10.0.0 по 10.0.16

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально созданных запросов.

**Последствия эксплуатации:** Выполнение произвольного кода

10 **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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://github.com/glpi-project/glpi/releases/tag/10.0.17>

**Краткое описание:** Получение конфиденциальной информации в GLPI

**Идентификатор уязвимости:** CVE-2024-47758

**Идентификатор программной ошибки:** CWE-284 Некорректное управление доступом

**Уязвимый продукт:** GLPI: с версии 10.0.0 по 10.0.16

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход ограничений безопасности

**Последствия эксплуатации:** Получение конфиденциальной информации

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://github.com/glpi-project/glpi/releases/tag/10.0.17>

**Краткое описание:** Обход безопасности в GLPI

**Идентификатор уязвимости:** CVE-2024-47761

**Идентификатор программной ошибки:** CWE-640 Ненадежный механизм восстановления забытого пароля

**Уязвимый продукт:** GLPI: с версии 10.0.0 по 10.0.16

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Обход безопасности

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://github.com/glpi-project/glpi/releases/tag/10.0.17>

**Краткое описание:** Получение конфиденциальной информации в GLPI

**Идентификатор уязвимости:** CVE-2024-47760

**Идентификатор программной ошибки:** CWE-284 Некорректное управление доступом

**Уязвимый продукт:** GLPI: с версии 10.0.0 по 10.0.16

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход ограничений безопасности

**Последствия эксплуатации:** Получение конфиденциальной информации

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://github.com/glpi-project/glpi/releases/tag/10.0.17>

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-50339  
BDU:2024-09128

Идентификатор программной ошибки: CWE-384 Фиксация сессии

Уязвимый продукт: GLPI: с версии 10.0.0 по 10.0.16

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-11-06 / 2024-11-06

Ссылки на источник:

- <http://github.com/glpi-project/glpi/releases/tag/10.0.17>
- <https://bdu.fstec.ru/vul/2024-09128>

**Краткое описание:** Перезапись произвольных файлов в ZipArchive

**Идентификатор уязвимости:** CVE-2022-36943

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

**Уязвимый продукт:** ZipArchive: 0.1.0 - 2.5.2

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Перезапись произвольных файлов

15 **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:N/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://github.com/metaredteam/external-disclosures/security/advisories/GHSA-vgww-6xcf-qqfc>

**Краткое описание:** Выполнение произвольного кода в Apache ZooKeeper

**Идентификатор уязвимости:** CVE-2024-51504

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

**Уязвимый продукт:** ZooKeeper: 3.9.0 - 3.9.2

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Обход процесса аутентификации

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-06 / 2024-11-06

**Ссылки на источник:**

- <http://lists.apache.org/thread/dgvx1vr8jy69d65lrs1357lqvmb4wfw6>

**Краткое описание:** Выполнение произвольного кода в Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Points

**Идентификатор уязвимости:** CVE-2024-20418  
BDU:2024-09127

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

**Уязвимый продукт:** Ultra-Reliable Wireless Backhaul: все версии  
Cisco Unified Industrial Wireless Software: 17.14 - 17.15  
Catalyst IW9165D Heavy Duty Access Points: все версии  
Catalyst IW9165E Rugged Access Points and Wireless Clients: все версии  
Catalyst IW9167E Heavy Duty Access Points: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

17 **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:** 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-07 / 2024-11-07

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs>
- <https://bdu.fstec.ru/vul/2024-09127>

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

**Идентификатор уязвимости:** CVE-2024-10827

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.93  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.68

**Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты

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

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-07 / 2024-11-07

**Ссылки на источник:**

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-10827>

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

**Идентификатор уязвимости:** CVE-2024-10826

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.93  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.68

**Категория уязвимого продукта:** Операционные системы Microsoft и их компоненты

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

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-11-07 / 2024-11-07

**Ссылки на источник:**

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-10826>

**Краткое описание:** Получение конфиденциальной информации в Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100 and 4200 Series

**Идентификатор уязвимости:** CVE-2024-20412  
BDU:2024-08575

**Идентификатор программной ошибки:** CWE-259 Использование жестко закодированного пароля

**Уязвимый продукт:** Cisco Firepower Threat Defense (FTD): 7.1.0 - 7.4.1.1  
Firepower 1000 Series Appliances: все версии  
Firepower 2100 Series Security Appliances: все версии  
Firepower 3100 Series Appliances: все версии  
Firepower 4200 Series Appliances: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Использование жестко закодированного пароля

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5>
- <https://bdu.fstec.ru/vul/2024-08575>

**Краткое описание:** Выполнение произвольного кода в Cisco Adaptive Security Appliance Software

**Идентификатор уязвимости:** CVE-2024-20329

**Идентификатор программной ошибки:** CWE-146 Некорректная нейтрализация разделителей выражений или команд

**Уязвимый продукт:** Cisco Adaptive Security Appliance (ASA): 9.17.1 - 9.19.1.18

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Некорректная проверка входных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF>
- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-M446vbEO>
- <http://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75300>