

# 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.2024-10-28.1 | 28 октября 2024 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-21810	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
2	Высокая	CVE-2024-23497	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
3	Высокая	CVE-2024-23981	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
4	Высокая	CVE-2024-24986	Dell APEX Cloud Platform for Microsoft Azure	Локальный	PE	2024-10-25	✓
5	Высокая	CVE-2024-21807	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
6	Высокая	CVE-2023-31102	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
7	Высокая	CVE-2023-40481	Dell APEX Cloud Platform for Microsoft Azure	Локальный	ACE	2024-10-25	✓
8	Высокая	CVE-2023-41833	Dell APEX Cloud Platform for Microsoft Azure	Локальный	PE	2024-10-25	✓
9	Критическая	CVE-2024-38474	Dell CyberSense OS	Сетевой	ACE	2024-10-25	✓
10	Критическая	CVE-2024-38476	Dell CyberSense OS	Сетевой	CSRF	2024-10-25	✓
11	Высокая	CVE-2024-38477	Dell CyberSense OS	Сетевой	DoS	2024-10-25	✓

12	Высокая	CVE-2024-39573	Dell CyberSense OS	Сетевой	CSRF	2024-10-25	✓
13	Высокая	CVE-2024-38473	Dell CyberSense OS	Сетевой	OSI	2024-10-25	✓
14	Критическая	CVE-2024-38475	Dell CyberSense OS	Сетевой	ACE	2024-10-25	✓
15	Критическая	CVE-2024-47575	Fortinet FortiManager	Сетевой	OSI	2024-10-23	✓
16	Критическая	CVE-2024-20424	Cisco Secure Firewall Management Center	Сетевой	ACE	2024-10-24	✓
17	Высокая	CVE-2024-20495	Cisco Adaptive Security Appliance and Firepower Threat Defense Software	Сетевой	DoS	2024-10-24	✓
18	Высокая	CVE-2024-20330	Cisco Firepower Threat Defense Software for Cisco Firepower 2100 Series Appliances	Сетевой	DoS	2024-10-25	✓
19	Высокая	CVE-2024-20339	Cisco Firepower Threat Defense Software for Firepower 2100 Series	Сетевой	DoS	2024-10-25	✓
20	Высокая	CVE-2024-20426	Cisco Adaptive Security Appliance and Firepower Threat Defense Software	Сетевой	DoS	2024-10-25	✓
21	Высокая	CVE-2024-20260	Cisco Adaptive Security Virtual Appliance and Secure Firewall Threat Defense Virtual	Сетевой	DoS	2024-10-25	✓
22	Высокая	CVE-2024-10231	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-23	✓
23	Высокая	CVE-2024-10230	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-23	✓
24	Высокая	CVE-2024-41311	Libheif	Сетевой	ACE	2024-10-23	✓

25	Высокая	CVE-2024-10229	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-10-23	✓
26	Высокая	CVE-2024-20402	Cisco Adaptive Security Appliance and Firepower Threat Defense Software SSL VPN	Сетевой	DoS	2024-10-23	✓
27	Высокая	CVE-2024-8312	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	XSS\CSS	2024-10-25	✓
28	Высокая	CVE-2024-20351	Cisco Firepower Threat Defense Software and Cisco FirePOWER Services	Сетевой	DoS	2024-10-23	✓

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2024-21810  
BDU:2024-07406

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

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 8.8 AV:L/AC:L/PR:L/UI:N/S: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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-07406>

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2024-23497

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Переполнение буфера.

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 8.8 AV:L/AC:L/PR:L/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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2024-23981

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

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

**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:** 8.8 AV:L/AC:L/PR:L/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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>

**Краткое описание:** Повышение привилегий в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2024-24986

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

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до версии 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Повышение привилегий

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:L/AC:L/PR:L/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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2024-21807  
BDU:2024-07407

**Идентификатор программной ошибки:** CWE-665 Некорректная инициализация

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до версии 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**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:** 8.8 AV:L/AC:L/PR:L/UI:N/S: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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-07407>

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2023-31102  
BDU:2023-04942

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

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до версии 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 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:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>
- <https://bdu.fstec.ru/vul/2023-04942>

**Краткое описание:** Выполнение произвольного кода в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2023-40481  
BDU:2023-04886

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до версии 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

7

**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:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>
- <https://bdu.fstec.ru/vul/2023-04886>

**Краткое описание:** Повышение привилегий в Dell APEX Cloud Platform for Microsoft Azure

**Идентификатор уязвимости:** CVE-2023-41833

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

**Уязвимый продукт:** APEX Cloud Platform for Microsoft Azure: до версии 01.03.00.00

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированного запроса.

**Последствия эксплуатации:** Повышение привилегий

8 **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:L/AC:H/PR:H/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://www.dell.com/support/kbdoc/nl-nl/000237607/dsa-2024-416-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities>

**Краткое описание:** Выполнение произвольного кода в Dell CyberSense OS

**Идентификатор уязвимости:** CVE-2024-38474  
BDU:2024-06593

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

**Уязвимый продукт:** CyberSense OS: до 1.5.0-47

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

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

**Последствия эксплуатации:** Выполнение произвольного кода

9

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

**Оценка CVSSv3:** 9.8 AV:N/AC:L/PR:N/UI:N/S:U/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://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-06593>

**Краткое описание:** Подделка запросов на стороне сервера в Dell CyberSense OS

**Идентификатор уязвимости:** CVE-2024-38476  
BDU:2024-05131

**Идентификатор программной ошибки:** CWE-918 Подделка запроса со стороны сервера

**Уязвимый продукт:** CyberSense OS: до версии 1.5.0-47

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

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Подделка запросов на стороне сервера

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:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

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

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-05131>

**Краткое описание:** Отказ в обслуживании в Dell CyberSense OS

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

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

**Уязвимый продукт:** CyberSense OS: до версии 1.5.0-47

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

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

**Последствия эксплуатации:** Отказ в обслуживании

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:** 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:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-05195>

**Краткое описание:** Подделка запросов на стороне сервера в Dell CyberSense OS

**Идентификатор уязвимости:** CVE-2024-39573  
BDU:2024-05631

**Идентификатор программной ошибки:** CWE-918 Подделка запроса со стороны сервера

**Уязвимый продукт:** CyberSense OS: до версии 1.5.0-47

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

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

**Последствия эксплуатации:** Подделка запросов на стороне сервера

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:** 7.5 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:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-05631>

**Краткое описание:** Получение конфиденциальной информации в Dell CyberSense OS

**Идентификатор уязвимости:** CVE-2024-38473  
BDU:2024-06893

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

**Уязвимый продукт:** CyberSense OS: до версии 1.5.0-47

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

**Способ эксплуатации:** Обход процесса аутентификации

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

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

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-06893>

**Краткое описание:** Выполнение произвольного кода в Dell CyberSense OS

**Идентификатор уязвимости:** CVE-2024-38475  
BDU:2024-04936

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

**Уязвимый продукт:** CyberSense OS: до версии 1.5.0-47

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

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

**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:** 9.1 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:** 2024-10-25 / 2024-10-25

**Ссылки на источник:**

- <http://www.dell.com/support/kbdoc/nl-nl/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities>
- <https://bdu.fstec.ru/vul/2024-04936>

**Краткое описание:** Получение конфиденциальной информации в Fortinet FortiManager

**Идентификатор уязвимости:** CVE-2024-47575  
BDU:2024-08556

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

**Уязвимый продукт:** FortiManager: с версии 6.2.0 по 7.6.0

**Категория уязвимого продукта:** Средства защиты информации

**Способ эксплуатации:** Отправка специально сформированного запроса.

**Последствия эксплуатации:** Получение конфиденциальной информации

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:** 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:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- <http://www.fortiguard.com/psirt/FG-IR-24-423>
- <https://bdu.fstec.ru/vul/2024-08556>

**Краткое описание:** Выполнение произвольного кода в Cisco Secure Firewall Management Center

**Идентификатор уязвимости:** CVE-2024-20424

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

**Уязвимый продукт:** Cisco Secure Firewall Management Center (formerly Firepower Management Center, FMC): с версии 6.4.0 по 7.4.1.1

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**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:** 9.9 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:** 2024-10-24 / 2024-10-24

**Ссылки на источник:**

- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj68540>

**Краткое описание:** Отказ в обслуживании в Cisco Adaptive Security Appliance and Firepower Threat Defense Software

**Идентификатор уязвимости:** CVE-2024-20495

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

**Уязвимый продукт:** Cisco Adaptive Security Appliance и Firepower Threat Defense Software:  
Cisco ASA: с версии 6.2.3.16 по 9.17.1.39  
Cisco FTD: с версии 6.2.3.16 по 9.17.1.39

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-24 / 2024-10-24

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-cZf8gT>

**Краткое описание:** Отказ в обслуживании в Cisco Firepower Threat Defense Software for Cisco Firepower 2100 Series Appliances

**Идентификатор уязвимости:** CVE-2024-20330

**Идентификатор программной ошибки:** CWE-788 Доступ к областям памяти за пределами буфера

**Уязвимый продукт:** Cisco Firepower Threat Defense:  
Cisco FTD: с версии 7.0.0 по 7.4.1.1  
Firepower 2100 Series Security Appliances: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** Отказ в обслуживании

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

**Оценка CVSSv3:** 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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-ftd2100-snort-dos-M9HuMt75>
- <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>

**Краткое описание:** Отказ в обслуживании в Cisco Firepower Threat Defense Software for Firepower 2100 Series

**Идентификатор уязвимости:** CVE-2024-20339

**Идентификатор программной ошибки:** CWE-476 Разыменование нулевого указателя

**Уязвимый продукт:** Cisco Firepower Threat Defense Software:  
Cisco FTD: с версии 6.2.3 по 7.3.1.2  
Firepower 2100 Series Firewalls: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** Отказ в обслуживании

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

**Оценка CVSSv3:** 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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-ftd-tls-dos-QXYE5Ufy>
- <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>

**Краткое описание:** Отказ в обслуживании в Cisco Adaptive Security Appliance and Firepower Threat Defense Software

**Идентификатор уязвимости:** CVE-2024-20426

**Идентификатор программной ошибки:** CWE-476 Разыменование нулевого указателя

**Уязвимый продукт:** Cisco Adaptive Security Virtual Appliance и Cisco Firepower Threat Defense Virtual:  
Cisco ASA: с версии 7.2.0 по 9.20.2.21  
Cisco FTDv: с версии 7.2.0 по 9.20.2.21

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**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:** 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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-asaftd-ikev2-dos-9FgEyHsF>

**Краткое описание:** Отказ в обслуживании в Cisco Adaptive Security Virtual Appliance and Secure Firewall Threat Defense Virtual

**Идентификатор уязвимости:** CVE-2024-20260

**Идентификатор программной ошибки:** CWE-789 Неконтролируемое выделение памяти

**Уязвимый продукт:** Cisco Adaptive Security Virtual Appliance и Cisco Firepower Threat Defense Virtual:  
Cisco ASAv: с версии 6.2.3 по 9.20.2.21  
Cisco FTDv: с версии 6.2.3 по 9.20.2.21

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**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:** 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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-asaftdvirtual-dos-MuenGnYR>

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

**Идентификатор уязвимости:** CVE-2024-10231

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

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.59  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 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:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop\\_22.html](http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_22.html)
- <http://crbug.com/372269618>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-10231>

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

**Идентификатор уязвимости:** CVE-2024-10230

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

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.59  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

23 **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:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop\\_22.html](http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_22.html)
- <http://crbug.com/371565065>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-10230>

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

**Идентификатор уязвимости:** CVE-2024-41311

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** libheif: с версии 1.0.0 по 1.17.6

**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.

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- <http://github.com/strukturag/libheif/issues/1226>
- <http://github.com/strukturag/libheif/pull/1227>
- <http://github.com/strukturag/libheif/commit/a3ed1b1eb178c5d651d6ac619c8da3d71ac2be36>
- <http://gist.github.com/flyyee/79f1b224069842ee320115cafa5c35c0>

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

**Идентификатор уязвимости:** CVE-2024-10229

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

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.59  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.52

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Получение конфиденциальной информации

25 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop\\_22.html](http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_22.html)
- <http://crbug.com/371011220>
- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-10229>

**Краткое описание:** Отказ в обслуживании в Cisco Adaptive Security Appliance and Firepower Threat Defense Software SSL VPN

**Идентификатор уязвимости:** CVE-2024-20402

**Идентификатор программной ошибки:** CWE-788 Доступ к областям памяти за пределами буфера

**Уязвимый продукт:** Cisco Firepower Threat Defense (FTD): 7.0.0 - 7.0.6.2  
Cisco Adaptive Security Appliance (ASA): 9.8.0.56 - 9.19.1.37

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** Отказ в обслуживании

26

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-dos-hOnB9pH4>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb00494>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj82247>

**Краткое описание:** Межсайтовый скриптинг в GitLab Community Edition (CE) and Enterprise Edition (EE)

**Идентификатор уязвимости:** CVE-2024-8312

**Идентификатор программной ошибки:** CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

**Уязвимый продукт:** Gitlab Community Edition: 15.10.0 - 17.5.0  
GitLab Enterprise Edition: 15.10.0 - 17.5.0

**Категория уязвимого продукта:** Универсальные компоненты и библиотеки

**Способ эксплуатации:** Открытие пользователем специально созданной вредоносной ссылки.

**Последствия эксплуатации:** Межсайтовый скриптинг

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

**Оценка CVSSv3:** 8.7 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

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

**Ссылки на источник:**

- <http://gitlab.com/gitlab-org/gitlab/-/issues/481819>
- <http://hackerone.com/reports/2659386>

**Краткое описание:** Отказ в обслуживании в Cisco Firepower Threat Defense Software and Cisco FirePOWER Services

**Идентификатор уязвимости:** CVE-2024-20351

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

**Уязвимый продукт:** FirePOWER Services: все версии  
Cisco Firepower Threat Defense (FTD); до 7.6.0

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

**Последствия эксплуатации:** Отказ в обслуживании

28

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-23 / 2024-10-23

**Ссылки на источник:**

- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sa-ftd-snort-fw-BCJTZPMu>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh41094>
- <http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh14067>