НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-03-25.1 | 25 марта 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	None	RabbitMQ C client	Сетевой	ACE	2024-03-25	✓
2	Высокая	CVE-2023-42950	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-03-25	✗
3	Высокая	CVE-2024-29944	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-03-22	✓
4	Высокая	CVE-2024-29943	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-03-22	✓
5	Высокая	CVE-2024-2387	Advanced Form Integration plugin for WordPress	Сетевой	ACE	2024-03-22	✓
6	Критическая	CVE-2024-29133	Apache Commons Configuration	Сетевой	ACE	2024-03-21	✓
7	Критическая	CVE-2024-29131	Apache Commons Configuration	Сетевой	ACE	2024-03-21	✓
8	Высокая	CVE-2024-22078	Elspec G5 digital fault recorder	Сетевой	PE	2024-03-21	✓
9	Высокая	CVE-2024-22082	Elspec G5 digital fault recorder	Сетевой	RLF	2024-03-21	✓
10	Критическая	CVE-2024-22083	Elspec G5 digital fault recorder	Сетевой	ACE	2024-03-21	✓
11	Высокая	CVE-2024-22084	Elspec G5 digital fault recorder	Сетевой	OSI	2024-03-21	✓
12	Критическая	CVE-2024-22081	Elspec G5 digital fault recorder	Сетевой	ACE	2024-03-21	✓
13	Критическая	CVE-2024-22080	Elspec G5 digital fault recorder	Сетевой	ACE	2024-03-21	✓

14	Высокая	CVE-2024-22079	Elspec G5 digital fault recorder	Сетевой	RLF	2024-03-21	✓
15	Критическая	CVE-2024-28179	Jupyter Server Proxy	Сетевой	ACE	2024-03-20	✓
16	Высокая	CVE-2024-20327	Cisco IOS XR Software for ASR 9000 Series Aggregation Services Routers	Смежная сеть	DoS	2024-03-14	✓
17	Высокая	CVE-2024-20318	Cisco IOS XR Software	Смежная сеть	DoS	2024-03-14	✓
18	Высокая	CVE-2024-20320	Cisco IOS XR Software	Локальный	PE	2024-03-14	✓
19	Высокая	CVE-2023-46717	FortiOS	Сетевой	SB	2024-03-12	✓
20	Высокая	CVE-2023-23112	FortiOS	Смежная сеть	OSI	2024-03-12	✓

1

Краткое описание: Выполнение произвольного кода в RabbitMQ C client

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: RabbitMQ C client: 0.1 - 0.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-25 / 2024-03-25

Ссылки на источник:

- http://github.com/alanxz/rabbitmq-c/releases/tag/v0.14.0

2

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

Идентификатор уязвимости: CVE-2023-42950

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

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:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-25 / 2024-03-25

Ссылки на источник:

- http://support.apple.com/en-us/HT214036

3

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-29944

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Mozilla Firefox: 100.0 - 124.0
Firefox ESR: 102.0 - 115.9.0

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-22 / 2024-03-22

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-15/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-16/

4

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-29943

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Mozilla Firefox: 116.0 - 124.0

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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-22 / 2024-03-22

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-15/

5

Краткое описание: Выполнение произвольного кода в Advanced Form Integration plugin for WordPress

Идентификатор уязвимости: CVE-2024-2387

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

Уязвимый продукт: Advanced Form Integration: 1..68.1 - 1.82.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-22 / 2024-03-22

Ссылки на источник:

- http://www.wordfence.com/threat-intel/vulnerabilities/id/45d5a677-9b8b-4258-9cfb-101b0f0e6f6f?source=cve
- http://plugins.trac.wordpress.org/browser/advanced-form-integration/trunk/includes/class-adfoin-log-table.php#L275
- http://plugins.trac.wordpress.org/browser/advanced-form-integration/trunk/includes/class-adfoin-log-table.php#L227
- http://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3052201%40advanced-form-integration&new=3052201%40advanced-form-integration&sfp_email=&sfph_mail=

6

Краткое описание: Выполнение произвольного кода в Apache Commons Configuration

Идентификатор уязвимости: CVE-2024-29133

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Apache Commons Configuration: 2.0 - 2.10.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://lists.apache.org/thread/ccb9w15bscznh6tnp3wsvrrj9crbszh2

Краткое описание: Выполнение произвольного кода в Apache Commons Configuration

Идентификатор уязвимости: CVE-2024-29131

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Apache Commons Configuration: 2.0 - 2.10.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://seclists.org/oss-sec/2024/q1/239

8

Краткое описание: Повышение привилегий в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22078

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

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Чтение локальных файлов в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22082

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

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Выполнение произвольного кода в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22083

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

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:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

11

Краткое описание: Получение конфиденциальной информации в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22084

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Выполнение произвольного кода в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22081

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

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Выполнение произвольного кода в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22080

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

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Чтение локальных файлов в Elspec G5 digital fault recorder

Идентификатор уязвимости: CVE-2024-22079

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

Уязвимый продукт: G5 digital fault recorder: 1.1.4.15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-21 / 2024-03-21

Ссылки на источник:

- http://www.elspec-ltd.com/support/security-advisories/

Краткое описание: Выполнение произвольного кода в Jupyter Server Proxy

Идентификатор уязвимости: CVE-2024-28179

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

Уязвимый продукт: Jupyter Server Proxy: 3.2.0 - 4.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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: 9.0 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: 2024-03-20 / 2024-03-20

Ссылки на источник:

- http://github.com/jupyterhub/jupyter-server-proxy/security/advisories/GHSA-w3vc-fx9p-wp4v

Краткое описание: Отказ в обслуживании в Cisco IOS XR Software for ASR 9000 Series Aggregation Services Routers

Идентификатор уязвимости: CVE-2024-20327

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco IOS XR: 7.8 - 7.11
Cisco ASR 9000 Series Aggregation Services Routers: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-14 / 2024-03-14

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pppma-JKWFgneW

17

Краткое описание: Отказ в обслуживании в Cisco IOS XR Software

Идентификатор уязвимости: CVE-2024-20318

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco IOS XR: 7.8 - 7.10
IOS XRd vRouter: все версии
Cisco IOS XRv 9000 Router: все версии
Cisco ASR 9000 Series Aggregation Services Routers: все версии
Cisco ASR 9006 Router: все версии
Cisco ASR 9010 Router: все версии
Cisco ASR 9901 Router: все версии
Cisco ASR 9902 Router: все версии
Cisco ASR 9903 Router: все версии
Cisco ASR 9904 Router: все версии
Cisco ASR 9906 Router: все версии
Cisco ASR 9910 Router: все версии
Cisco ASR 9912 Router: все версии
Cisco ASR 9922 Router: все версии

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-14 / 2024-03-14

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrl2vpn-jesrU3fc

- https://bdu.fstec.ru/vul/2024-02055

18

Краткое описание: Повышение привилегий в Cisco IOS XR Software

Идентификатор уязвимости: CVE-2024-20320

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Cisco IOS XR: для Cisco ASR серии 8000.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-14 / 2024-03-14

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ssh-privesc-eWDMKew3
- https://bdu.fstec.ru/vul/2024-01988

19

Краткое описание: Обход безопасности в FortiOS

Идентификатор уязвимости: CVE-2023-46717

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FortiOS: до версии 7.4.1

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

Способ эксплуатации: Обход процесса аутентификации

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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-12 / 2024-03-12

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-424
- https://bdu.fstec.ru/vul/2024-02007

Краткое описание: Получение конфиденциальной информации в FortiOS

Идентификатор уязвимости: CVE-2023-23112

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: FortiOS: до версии 7.4.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Получение конфиденциальной информации

20

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

Оценка CVSSv3: 8.0 AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-12 / 2024-03-15

Ссылки на источник: