

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-02-09.1 | 9 февраля 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-1329	HashiCorp Nomad	Сетевой	PE	2024-02-08	✓
2	Высокая	CVE-2024-21626	HashiCorp Nomad	Локальный	OSI	2024-02-08	✓
3	Высокая	CVE-2024-22024	Ivanti Connect Secure and Policy Secure	Сетевой	RLF	2024-02-09	✓
4	Высокая	CVE-2023-44487	FortiOS and FortiProxy	Сетевой	DoS	2024-02-09	✓
5	Критическая	CVE-2024-23113	FortiOS fgfmd	Сетевой	ACE	2024-02-09	✓
6	Критическая	CVE-2024-21762	FortiOS SSL-VPN	Сетевой	ACE	2024-02-09	✓
7	Высокая	CVE-2024-20255	Cisco Expressway Series and TelePresence Video Communication Server	Сетевой	CSRF	2024-02-08	✓
8	Критическая	CVE-2024-20254	Cisco Expressway Series and TelePresence Video Communication Server	Сетевой	CSRF	2024-02-08	✓
9	Критическая	CVE-2024-20252	Cisco Expressway Series and TelePresence Video Communication Server	Сетевой	CSRF	2024-02-08	✓
10	Высокая	CVE-2024-22394	SonicWall SonicOS SSL-VPN	Сетевой	SB	2024-02-08	✓
11	Высокая	CVE-2023-40547	UEFI shim loader	Смежная сеть	OSI	2024-02-07	✓

12	Высокая	CVE-2023-52138	Engrampa	Сетевой	ACE	2024-02-07	✓
13	Критическая	CVE-2023-5841	OpenEXR	Сетевой	ACE	2024-02-07	✗
14	Высокая	CVE-2024-20290	ClamAV	Сетевой	DoS	2024-02-07	✓
15	Критическая	CVE-2024-20328	ClamAV	Сетевой	ACE	2024-02-07	✓
16	Критическая	CVE-2024-23917	JetBrains TeamCity	Сетевой	ACE	2024-02-07	✓
17	Высокая	CVE-2024-1283	Google Chrome	Сетевой	ACE	2024-02-07	✓
18	Высокая	CVE-2024-1284	Google Chrome	Сетевой	ACE	2024-02-07	✓
19	Критическая	CVE-2024-0244	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
20	Критическая	CVE-2023-6234	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
21	Критическая	CVE-2023-6233	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
22	Критическая	CVE-2023-6232	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
23	Критическая	CVE-2023-6231	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
24	Критическая	CVE-2023-6230	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓

25	Критическая	CVE-2023-6229	Canon Europe Small Office Multifunction Printers and Laser Printers	Сетевой	ACE	2024-02-06	✓
26	Критическая	CVE-2023-7077	Sharp NEC Display Solutions Public Displays	Сетевой	ACE	2024-02-06	✓
27	Высокая	CVE-2024-23214	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-02-06	✗
28	Высокая	CVE-2023-22819	Western Digital My Cloud OS 5, My Cloud Home and SanDisk ibi devices	Сетевой	DoS	2024-02-06	✓
29	Высокая	CVE-2023-22817	Western Digital My Cloud OS 5, My Cloud Home and SanDisk ibi devices	Сетевой	CSRF	2024-02-06	✓
30	Критическая	CVE-2024-22651	D-Link DIR-815	Сетевой	DoS	2024-01-24	✓
31	Критическая	CVE-2024-0541	Tenda W9	Сетевой	DoS	2024-01-15	✗
32	Критическая	CVE-2024-0540	Tenda W9	Сетевой	DoS	2024-01-15	✗
33	Критическая	CVE-2024-0538	Tenda W9	Сетевой	DoS	2024-01-14	✗
34	Критическая	CVE-2024-0537	Tenda W9	Сетевой	DoS	2024-01-14	✗
35	Критическая	CVE-2024-0536	Tenda W9	Сетевой	DoS	2024-01-14	✗
36	Высокая	CVE-2024-21620	Juniper Junos OS	Сетевой	XSS\CSS	2024-01-26	✓

Краткое описание: Повышение привилегий в HashiCorp Nomad

Идентификатор уязвимости: CVE-2024-1329

Идентификатор программной ошибки: CWE-61 Уязвимости, связанные с символическими ссылками UNIX

Уязвимый продукт: Nomad Enterprise: с версии 1.0.0 по 1.7.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://github.com/hashicorp/nomad/releases/tag/v1.5.14>
- <http://github.com/hashicorp/nomad/issues/19888>
- <http://github.com/hashicorp/nomad/releases/tag/v1.6.7>
- <http://github.com/hashicorp/nomad/releases/tag/v1.7.4>

Краткое описание: Получение конфиденциальной информации в HashiCorp Nomad

Идентификатор уязвимости: CVE-2024-21626

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Nomad Enterprise: с версии 1.0.0 по 1.7.3

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://github.com/hashicorp/nomad/releases/tag/v1.5.14>
- <http://github.com/hashicorp/nomad/releases/tag/v1.6.7>
- <http://github.com/hashicorp/nomad/releases/tag/v1.7.4>
- <https://bdu.fstec.ru/vul/2024-00973>

Краткое описание: Чтение локальных файлов в Ivanti Connect Secure and Policy Secure

Идентификатор уязвимости: CVE-2024-22024

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Pulse Connect Secure and Pulse Policy Secure:
Pulse Connect Secure: до версии 22.6R2.2
Pulse Policy Secure: до версии 22.5R1.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: чтение 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: 8.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

Краткое описание: Отказ в обслуживании в FortiOS and FortiProxy

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: FortiProxy и FortiOS:
FortiProxy: с версии 7.0.0 по 7.4.1
FortiOS: с версии 7.0.0 по 7.4.2

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

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2024-02-09 / 2024-02-09

Ссылки на источник:

- <http://www.fortiguard.com/psirt/FG-IR-23-397>
- <https://bdu.fstec.ru/vul/2023-06559>

Краткое описание: Выполнение произвольного кода в FortiOS fgfmd

Идентификатор уязвимости: CVE-2024-23113

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: FortiOS: с версии 7.0.0 по 7.4.2

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

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-02-09 / 2024-02-09

Ссылки на источник:

- <http://www.fortiguard.com/psirt/FG-IR-24-029>

Краткое описание: Выполнение произвольного кода в FortiOS SSL-VPN

Идентификатор уязвимости: CVE-2024-21762

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FortiOS: с версии 6.0.0 по 7.4.2

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 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: 2024-02-09 / 2024-02-09

Ссылки на источник:

- <http://www.fortiguard.com/psirt/FG-IR-24-015>

Краткое описание: Подделка запросов на стороне сервера в Cisco Expressway Series and TelePresence Video Communication Server

Идентификатор уязвимости: CVE-2024-20255

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

Уязвимый продукт: Expressway Series: 14.0
Cisco TelePresence Video Communication Server: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Последствия эксплуатации: подделка запросов на стороне сервера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3>

Краткое описание: Подделка запросов на стороне сервера в Cisco Expressway Series and TelePresence Video Communication Server

Идентификатор уязвимости: CVE-2024-20254

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

Уязвимый продукт: Expressway Series: 14.0

Cisco TelePresence Video Communication Server: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Последствия эксплуатации: подделка запросов на стороне сервера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3>

Краткое описание: Подделка запросов на стороне сервера в Cisco Expressway Series and TelePresence Video Communication Server

Идентификатор уязвимости: CVE-2024-20252

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

Уязвимый продукт: Expressway Series: 14.0
Cisco TelePresence Video Communication Server: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Последствия эксплуатации: подделка запросов на стороне сервера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3>

Краткое описание: Обход безопасности в SonicWall SonicOS SSL-VPN

Идентификатор уязвимости: CVE-2024-22394

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: SonicOS: 7.1.1-7040

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

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-08 / 2024-02-08

Ссылки на источник:

- <http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0003>

Краткое описание: Получение конфиденциальной информации в UEFI shim loader

Идентификатор уязвимости: CVE-2023-40547

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Shim: 0.3 - 15.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://access.redhat.com/security/cve/CVE-2023-40547>
- http://bugzilla.redhat.com/show_bug.cgi?id=2234589
- <http://www.openwall.com/lists/oss-security/2024/01/26/1>
- <https://bdu.fstec.ru/vul/2024-00725>

Краткое описание: Выполнение произвольного кода в Engrampa

Идентификатор уязвимости: CVE-2023-52138

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

Уязвимый продукт: engrampa: 1.12.0 - 1.27.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://github.com/mate-desktop/engrampa/security/advisories/GHSA-c98h-v39w-3r7v>
- <http://github.com/mate-desktop/engrampa/commit/63d5dfa9005c6b16d0f0ccd888cc859fca78f970>

Краткое описание: Выполнение произвольного кода в OpenEXR

Идентификатор уязвимости: CVE-2023-5841

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

Уязвимый продукт: OpenEXR: 3.0.0 beta - 3.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://takeonme.org/cves/CVE-2023-5841.html>

14

Краткое описание: Отказ в обслуживании в ClamAV

Идентификатор уязвимости: CVE-2024-20290

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

Уязвимый продукт: ClamAV: 1.0.0 - 1.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-hDffu6t>
- <http://github.com/Cisco-Talos/clamav-devel/releases/tag/clamav-1.0.5>
- <http://blog.clamav.net/2023/11/clamav-130-122-105-released.html>
- <http://github.com/Cisco-Talos/clamav-devel/releases/tag/clamav-1.2.2>

Краткое описание: Выполнение произвольного кода в ClamAV

Идентификатор уязвимости: CVE-2024-20328

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

Уязвимый продукт: ClamAV: 1.0.0 - 1.2.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

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: 9.8 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: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://blog.clamav.net/2023/11/clamav-130-122-105-released.html>
- <http://github.com/Cisco-Talos/clamav-devel/releases/tag/clamav-1.0.5>
- <http://github.com/Cisco-Talos/clamav-devel/releases/tag/clamav-1.2.2>

Краткое описание: Выполнение произвольного кода в JetBrains TeamCity

Идентификатор уязвимости: CVE-2024-23917

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: TeamCity: 2017.1 - 2023.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса авторизации

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: 9.8 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: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://blog.jetbrains.com/teamcity/2024/02/critical-security-issue-affecting-teamcity-on-premises-cve-2024-23917/>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-1283

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.140

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

17

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: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html>
- <http://crbug.com/41494860>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-1284

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 121.0.6167.140

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

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: 8.8 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: 2024-02-07 / 2024-02-07

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html>
- <http://crbug.com/41494539>

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2024-0244

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

19

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6234

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

20

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6233

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

21

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6232

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

22

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6231

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

23

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6230

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

24

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Canon Europe Small Office Multifunction Printers and Laser Printers

Идентификатор уязвимости: CVE-2023-6229

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: i-SENSYS X C1333P: все версии
i-SENSYS X C1333iF: все версии
i-SENSYS X C1333i: все версии
i-SENSYS MF754Cdw: все версии
i-SENSYS MF752Cdw: все версии
i-SENSYS LBP673Cdw: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

25

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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.canon-europe.com/support/product-security-latest-news/>
- http://canon.a.bigcontent.io/v1/static/CPE2024-001_SmallOfficeMultifunctionPrintersAndLaserPrinters_AffectedModels_20240126

Краткое описание: Выполнение произвольного кода в Sharp NEC Display Solutions Public Displays

Идентификатор уязвимости: CVE-2023-7077

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

Уязвимый продукт: P403: все версии
P463: все версии
P553: все версии
P703: все версии
P801: все версии
X554UN: все версии
X464UN: все версии
X554UNS: все версии
X464UNV: все версии
X474HB: все версии
X464UNS: все версии
X554UNV: все версии
X555UNS: все версии
X555UNV: все версии
X754HB: все версии
X554HB: все версии
E705: все версии
E805: все версии
E905: все версии
UN551S: все версии
UN551VS: все версии
X551UHD: все версии
X651UHD: все версии
X841UHD: все версии
X981UHD: все версии
MD551C8: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2024-02-06 / 2024-02-06

Ссылки на источник:

- http://www.sharp-nec-displays.com/global/support/info/A4_vulnerability.html
- <http://jvn.jp/en/vu/JVNVU97836276/index.html>

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

Идентификатор уязвимости: CVE-2024-23214

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

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

27

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://support.apple.com/en-us/HT214061>

Краткое описание: Отказ в обслуживании в Western Digital My Cloud OS 5, My Cloud Home and SanDisk ibi devices

Идентификатор уязвимости: CVE-2023-22819

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

Уязвимый продукт: My Cloud PR2100: до 5.27.161
My Cloud PR4100: до 5.27.161
My Cloud EX4100: до 5.27.161
My Cloud EX2 Ultra: до 5.27.161
My Cloud Mirror G2: до 5.27.161
My Cloud DL2100: до 5.27.161
My Cloud DL4100: до 5.27.161
My Cloud EX2100: до 5.27.161
My Cloud (Glacier): до 5.27.161
WD Cloud: до 5.27.161
My Cloud Home: до 9.5.1-104
My Cloud Home Duo: до 9.5.1-104
SanDisk ibi: до 9.5.1-104

28

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.westerndigital.com/support/product-security/wdc-24001-western-digital-my-cloud-os-5-my-cloud-home-duo-and-sandisk-ibi-firmware-update>

- <http://www.zerodayinitiative.com/advisories/ZDI-24-088/>

Краткое описание: Подделка запросов на стороне сервера в Western Digital My Cloud OS 5, My Cloud Home and SanDisk ibi devices

Идентификатор уязвимости: CVE-2023-22817

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

Уязвимый продукт: My Cloud PR2100: до 5.27.161
My Cloud PR4100: до 5.27.161
My Cloud EX4100: до 5.27.161
My Cloud EX2 Ultra: до 5.27.161
My Cloud Mirror G2: до 5.27.161
My Cloud DL2100: до 5.27.161
My Cloud DL4100: до 5.27.161
My Cloud EX2100: до 5.27.161
My Cloud (Glacier): до 5.27.161
WD Cloud: до 5.27.161
My Cloud Home: до 9.5.1-104
My Cloud Home Duo: до 9.5.1-104
SanDisk ibi: до 9.5.1-104

29

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: подделка запросов на стороне сервера

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:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-06 / 2024-02-06

Ссылки на источник:

- <http://www.westerndigital.com/support/product-security/wdc-24001-western-digital-my-cloud-os-5-my-cloud-home-duo-and-sandisk-ibi-firmware-update>

- <http://www.zerodayinitiative.com/advisories/ZDI-24-087/>

Краткое описание: Отказ в обслуживании в D-Link DIR-815

Идентификатор уязвимости: CVE-2024-22651

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

Уязвимый продукт: D-Link DIR-815: до версии 1.04.

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.

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: 2024-01-24 / 2024-01-30

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0541

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: до версии 1.0.0.7(4456)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-01-15 / 2024-01-19

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-00936>

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0540

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: до версии 1.0.0.7(4456)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-01-15 / 2024-01-19

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-00941>

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0538

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: до версии 1.0.0.7(4456)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-01-14 / 2024-01-19

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-00939>

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: до версии 1.0.0.7(4456)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-01-14 / 2024-01-19

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-00946>

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0536

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: до версии 1.0.0.7(4456)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-01-14 / 2024-01-19

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-00937>

Краткое описание: Межсайтовый скриптинг в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21620

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

Уязвимый продукт: Juniper Junos OS: до 23.4R2

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

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: межсайтовый скриптинг

36

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: 2024-01-26 / 2024-01-26

Ссылки на источник:

- <http://supportportal.juniper.net/s/article/2024-01-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-have-been-addressed>
- <https://bdu.fstec.ru/vul/2024-00758>