НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-22.1 | 22 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-44808	D-Link	Сетевой	ACE	2023-10-16	✗
2	Высокая	CVE-2023-35127	Tellus Lite V-Simulator	Локальный	ACE	2023-11-22	✓
3	Критическая	CVE-2023-44809	D-Link	Сетевой	ACE	2023-10-16	✗
4	Критическая	CVE-2023-45575	D-Link	Сетевой	ACE	2023-10-16	✗
5	Критическая	CVE-2023-45572	D-Link	Сетевой	ACE	2023-10-16	✗
6	Критическая	CVE-2023-45576	D-Link	Сетевой	ACE	2023-10-16	✗
7	Критическая	CVE-2023-45574	D-Link	Сетевой	ACE	2023-10-16	✗
8	Критическая	CVE-2023-45578	D-Link	Сетевой	ACE	2023-10-16	✗
9	Критическая	CVE-2023-46536	TP-LINK	Сетевой	OSI	2023-10-23	✗
10	Критическая	CVE-2023-46538	TP-LINK	Сетевой	OSI	2023-10-23	✗
11	Критическая	CVE-2023-46539	TP-LINK	Сетевой	OSI	2023-10-23	✗
12	Критическая	CVE-2023-46537	TP-LINK	Сетевой	OSI	2023-10-23	✗
13	Критическая	CVE-2023-46534	TP-LINK	Сетевой	OSI	2023-10-23	✗

14	Критическая	CVE-2023-45577	D-Link	Сетевой	ACE	2023-10-16	✗
15	Критическая	CVE-2023-46370	Tenda W18E	Сетевой	ACE	2023-10-25	✗
16	Высокая	CVE-2023-44186	Junos Evolved и Junos OS	Сетевой	DoS	2023-10-17	✓
17	Высокая	CVE-2023-36841	Juniper Junos OS	Сетевой	DoS	2023-10-17	✓
18	Высокая	CVE-2023-44192	Juniper Junos OS	Сетевой	DoS	2023-10-17	✓
19	Высокая	CVE-2023-44197	Junos Evolved и Junos OS	Сетевой	DoS	2023-10-25	✓
20	Высокая	CVE-2023-44199	Juniper Junos OS	Сетевой	DoS	2023-10-17	✓
21	Высокая	CVE-2023-44191	Juniper Junos OS	Сетевой	DoS	2023-10-18	✓
22	Высокая	CVE-2023-44185	Junos Evolved и Junos OS	Сетевой	DoS	2023-10-16	✓
23	Высокая	CVE-2023-44181	Junos OS	Сетевой	DoS	2023-10-18	✓
24	Критическая	CVE-2023-31273	Intel Data Center Manager (DCM)	Сетевой	ACE	2023-11-21	✓
25	Критическая	CVE-2023-40151	Red Lion Sixnet RTUs	Сетевой	OSI	2023-11-21	✓
26	Критическая	CVE-2023-42770	Red Lion Sixnet RTUs	Сетевой	SB	2023-11-21	✓
27	Высокая	CVE-2023-39548	NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe	Сетевой	WLF	2023-11-21	✓
28	Высокая	CVE-2023-39547	NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe	Смежная сеть	SB	2023-11-21	✓

29	Высокая	CVE-2023-39544	NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe	Сетевой	ACE	2023-11-21	✓
30	Высокая	CVE-2023-26205	Fortinet FortiADC	Сетевой	PE	2023-11-20	✓
31	Высокая	CVE-2023-43622	Tenable SecurityCenter	Сетевой	DoS	2023-11-20	✓
32	Высокая	CVE-2023-5593	Zyxel SecuExtender SSL VPN client for Windows	Локальный	ACE	2023-11-21	✓

1

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-44808

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

Уязвимый продукт: D-Link:
dir-820l до версии 1.05b03

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-06943

2

Краткое описание: Выполнение произвольного кода в Tellus Lite V-Simulator

Идентификатор уязвимости: CVE-2023-35127

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tellus Lite V-Simulator: до 4.0.19.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-22 / 2023-11-22

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-325-02
- http://felib.fujielectric.co.jp/en/M10009/M20034/document_detail/c27d5b69-68ef-4af5-90ee-b5dab118f71a

3

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-44809

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: D-Link:
dir-820l до версии 1.05b03

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-06944

4

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45575

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07177

5

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45572

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07178

6

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45576

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07179

7

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45574

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07180

8

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45578

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07181

9

Краткое описание: Получение конфиденциальной информации в TP-LINK

Идентификатор уязвимости: CVE-2023-46536

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TP-LINK:
TL-WR886N до версии 7.0 3.0.14 Build 221115.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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: 2023-10-23 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07357

10

Краткое описание: Получение конфиденциальной информации в TP-LINK

Идентификатор уязвимости: CVE-2023-46538

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TP-LINK:
TL-WR886N до версии 7.0 3.0.14 Build 221115.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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: 2023-10-23 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07358

11

Краткое описание: Получение конфиденциальной информации в TP-LINK

Идентификатор уязвимости: CVE-2023-46539

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TP-LINK:
TL-WR886N до версии 7.0 3.0.14 Build 221115.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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: 2023-10-23 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07359

12

Краткое описание: Получение конфиденциальной информации в TP-LINK

Идентификатор уязвимости: CVE-2023-46537

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TP-LINK:
TL-WR886N до версии 7.0 3.0.14 Build 221115.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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: 2023-10-23 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07361

13

Краткое описание: Получение конфиденциальной информации в TP-LINK

Идентификатор уязвимости: CVE-2023-46534

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: TP-LINK:
TL-WR886N до версии 7.0 3.0.14 Build 221115.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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: 2023-10-23 / Не определено

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07360

14

Краткое описание: Выполнение произвольного кода в D-Link

Идентификатор уязвимости: CVE-2023-45577

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link:
DI-7003GV2, DI-7100G, DI-7100GV2, DI-7200G, DI-7200GV2, DI-7300G и DI-7400G до версии 23.08.25D1.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-16 / 2023-10-16

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07362

15

Краткое описание: Выполнение произвольного кода в Tenda W18E

Идентификатор уязвимости: CVE-2023-46370

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

Уязвимый продукт: Tenda W18E: до версии 16.01.0.8(1576).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-07477

Краткое описание: Отказ в обслуживании в Junos Evolved и Junos OS

Идентификатор уязвимости: CVE-2023-44186

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Junos Evolved и Junos OS:
Evolved до версии 23.2R2-EVO
OS до версии 23.2R2

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

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: 7.5 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: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-attempting-to-send-a-very-long-AS-PATH-to-a-non-4-byte-AS-capable-BGP-neighbor-CVE-2023-44186
- https://bdu.fstec.ru/vul/2023-06935

17

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36841

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Junos OS:
MX до версии 22.4R2

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-MX-Series-Receipt-of-malformed-TCP-traffic-will-cause-a-Denial-of-Service-CVE-2023-36841
- https://bdu.fstec.ru/vul/2023-06785

18

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-44192

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Junos OS:
QFX 5000 до версии 22.R3

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-QFX5000-Series-DMA-memory-leak-is-observed-when-specific-DHCP-packets-are-transmitted-over-pseudo-VTEP-CVE-2023-44192
- https://bdu.fstec.ru/vul/2023-07022

Краткое описание: Отказ в обслуживании в Junos Evolved и Junos OS

Идентификатор уязвимости: CVE-2023-44197

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Junos Evolved и Junos OS:
Evolved до версии 21.4R3-S5-EVO
OS до версии 21.4R3-S5

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

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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-rpd-crash-may-occur-when-BGP-is-processing-newly-learned-routes-CVE-2023-44197
- https://bdu.fstec.ru/vul/2023-07019

20

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-44199

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Juniper Junos OS:
MX Series до версии 22.2R2

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-MX-Series-In-a-PTP-scenario-a-prolonged-routing-protocol-churn-can-trigger-an-FPC-reboot-CVE-2023-44199
- https://bdu.fstec.ru/vul/2023-06836

21

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-44191

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Juniper Junos OS:
QFX 5000 и EX 4000 до версии 22.4R2

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-18 / 2023-10-18

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-QFX5000-Series-and-EX4000-Series-Denial-of-Service-DoS-on-a-large-scale-VLAN-due-to-PFE-hogging-CVE-2023-44191
- https://bdu.fstec.ru/vul/2023-06976

Краткое описание: Отказ в обслуживании в Junos Evolved и Junos OS

Идентификатор уязвимости: CVE-2023-44185

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Junos Evolved и Junos OS:
Evolved до версии 22.3R2-EVO
OS до версии 22.3R2

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2023-10-16 / 2023-10-16

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BGP-scenario-RPD-crashes-upon-receiving-and-processing-a-specific-malformed-ISO-VPN--BGP-UPDATE-packet-CVE-2023-44185
- https://bdu.fstec.ru/vul/2023-06974

23

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2023-44181

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

Уязвимый продукт: Junos OS:
QFX5k до версии 22.1R3

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-18 / 2023-10-18

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-QFX5k-l2-loop-in-the-overlay-impacts-the-stability-in-a-EVPN-VXLAN-environment-CVE-2023-44181
- https://bdu.fstec.ru/vul/2023-06841

Краткое описание: Выполнение произвольного кода в Intel Data Center Manager (DCM)

Идентификатор уязвимости: CVE-2023-31273

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Intel Data Center Manager (DCM): до 5.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00902.html

25

Краткое описание: Получение конфиденциальной информации в Red Lion Sixnet RTUs

Идентификатор уязвимости: CVE-2023-40151

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: Red Lion Sixnet RTUs:
ST-IPm-8460: 6.0.202
ST-IPm-6350: 4.9.114
VT-mIPm-135-D: 4.9.114
VT-mIPm-245-D: 4.9.114
VT-IPm2m-213-D: 4.9.114
VT-IPm2m-113-D: 4.9.114

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-320-01
- http://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution

Краткое описание: Обход безопасности в Red Lion Sixnet RTUs

Идентификатор уязвимости: CVE-2023-42770

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Red Lion Sixnet RTUs:
ST-IPm-8460: 6.0.202
ST-IPm-6350: 4.9.114
VT-mIPm-135-D: 4.9.114
VT-mIPm-245-D: 4.9.114
VT-IPm2m-213-D: 4.9.114
VT-IPm2m-113-D: 4.9.114

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

26

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-320-01
- http://
- http://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution

Краткое описание: Запись локальных файлов в NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe

Идентификатор уязвимости: CVE-2023-39548

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

Уязвимый продукт: NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe:
EXPRESSCLUSTER X: 1.0 - 5.1
EXPRESSCLUSTER X SingleServerSafe: 1.0 - 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://jpn.nec.com/security-info/secinfo/nv23-009_en.html
- http://jvn.jp/en/vu/JVNVU98954968/index.html

Краткое описание: Обход безопасности в NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe

Идентификатор уязвимости: CVE-2023-39547

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe:
EXPRESSCLUSTER X: 1.0 - 5.1
EXPRESSCLUSTER X SingleServerSafe: 1.0 - 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://jpn.nec.com/security-info/secinfo/nv23-009_en.html
- http://jvn.jp/en/vu/JVNVU98954968/index.html

Краткое описание: Выполнение произвольного кода в NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe

Идентификатор уязвимости: CVE-2023-39544

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: NEC Corporation EXPRESSCLUSTER X and EXPRESSCLUSTER SingleServerSafe:
EXPRESSCLUSTER X: 1.0 - 5.1
EXPRESSCLUSTER X SingleServerSafe: 1.0 - 5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

29

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://jpn.nec.com/security-info/secinfo/nv23-009_en.html
- http://jvn.jp/en/vu/JVNVU98954968/index.html

Краткое описание: Повышение привилегий в Fortinet FortiADC

Идентификатор уязвимости: CVE-2023-26205

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Fortinet FortiADC: 6.1.0 - 7.1.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: повышение привилегий

30 **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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-22-292

31

Краткое описание: Отказ в обслуживании в Tenable SecurityCenter

Идентификатор уязвимости: CVE-2023-43622

Идентификатор программной ошибки: CWE-399 Уязвимости, связанные с управлением ресурсами

Уязвимый продукт: Tenable SecurityCenter: 6.0.0 - SC-202310.1

Категория уязвимого продукта: Средства защиты информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://www.tenable.com/security/tns-2023-42
- https://bdu.fstec.ru/vul/2023-07171

32

Краткое описание: Выполнение произвольного кода в Zyxel SecuExtender SSL VPN client for Windows

Идентификатор уязвимости: CVE-2023-5593

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Zyxel SecuExtender SSL VPN client for Windows: 4.0.4.0

Категория уязвимого продукта: Средства защиты информации

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: 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: 2023-11-21 / 2023-11-21

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-vulnerability-in-secuextender-ssl-vpn-client-software