НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-17.1 | 17 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-22527	Atlassian Confluence Data Center and Server	Сетевой	ACE	2024-01-16	✓
2	Критическая	CVE-2024-21591	Juniper Junos OS	Сетевой	ACE	2024-01-10	✓
3	Критическая	CVE-2024-21591	Juniper Junos OS	Сетевой	ACE	2024-01-10	✓
4	Высокая	CVE-2023-24329	Juniper Networks Session Smart Router	Сетевой	SB	2024-01-12	✓
5	Высокая	CVE-2023-32067	Juniper Networks Session Smart Router	Сетевой	DoS	2024-01-12	✓
6	Высокая	CVE-2023-2828	Juniper Networks Session Smart Router	Сетевой	DoS	2024-01-12	✓
7	Критическая	CVE-2023-38408	Juniper Networks Session Smart Router	Сетевой	ACE	2024-01-12	✓
8	Высокая	CVE-2023-3341	Juniper Networks Session Smart Router	Сетевой	DoS	2024-01-12	✓
9	Высокая	CVE-2023-38802	Juniper Networks Session Smart Router	Сетевой	DoS	2024-01-12	✓
10	Высокая	CVE-2023-1281	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓
11	Высокая	CVE-2023-1829	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓
12	Высокая	CVE-2023-2124	Juniper Networks Session Smart Router	Локальный	DoS	2024-01-12	✓
13	Высокая	CVE-2023-2235	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓

14	Высокая	CVE-2023-0266	Juniper Networks Session Smart Router	Смежная сеть	ACE	2024-01-12	✓
15	Высокая	CVE-2023-0386	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓
16	Высокая	CVE-2023-23918	Juniper Networks Session Smart Router	Сетевой	SB	2024-01-12	✓
17	Высокая	CVE-2023-0767	Juniper Networks Session Smart Router	Сетевой	ACE	2024-01-12	✓
18	Высокая	CVE-2023-22809	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓
19	Высокая	CVE-2023-0461	Juniper Networks Session Smart Router	Локальный	PE	2024-01-12	✓
20	Высокая	CVE-2023-51628	D-Link DCS-8300LHV2	Смежная сеть	ACE	2024-01-15	✓
21	Высокая	CVE-2023-51626	D-Link DCS-8300LHV2	Смежная сеть	ACE	2024-01-15	✓
22	Высокая	CVE-2023-51625	D-Link DCS-8300LHV2	Смежная сеть	ACE	2024-01-15	✓
23	Высокая	CVE-2023-51624	D-Link DCS-8300LHV2	Смежная сеть	ACE	2024-01-15	✓
24	Высокая	CVE-2023-51627	D-Link DCS-8300LHV2	Смежная сеть	ACE	2024-01-15	✓

Краткое описание: Выполнение произвольного кода в Atlassian Confluence Data Center and Server

Идентификатор уязвимости: CVE-2023-22527

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

Уязвимый продукт: Atlassian Confluence Server: 8.0.0 - 8.5.3
Confluence Data Center: 8.0.0 - 8.5.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-16 / 2024-01-16

Ссылки на источник:

- http://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
- http://jira.atlassian.com/browse/CONFSERVER-93833

2

Краткое описание: Выполнение произвольного кода в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21591

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Juniper Junos OS: 20.4R1 - 22.4R2-S1

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591
- https://bdu.fstec.ru/vul/2024-00263

3

Краткое описание: Выполнение произвольного кода в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21591

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Juniper Junos OS: 20.4R1 - 22.4R2-S1

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591
- https://bdu.fstec.ru/vul/2024-00263

4

Краткое описание: Обход безопасности в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-24329

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-04978

5

Краткое описание: Отказ в обслуживании в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-32067

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных DNS-запросов.

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-07649

6

Краткое описание: Отказ в обслуживании в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-2828

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

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-07642

7

Краткое описание: Выполнение произвольного кода в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-38408

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-03950

8

Краткое описание: Отказ в обслуживании в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-3341

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

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-06079

9

Краткое описание: Отказ в обслуживании в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-38802

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-05649

10

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-1281

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-01571

11

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-1829

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-02165

12

Краткое описание: Отказ в обслуживании в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-2124

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 7.8 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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-02529

13

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-2235

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-02407

14

Краткое описание: Выполнение произвольного кода в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-0266

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-00382

15

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-0386

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

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-01572

16

Краткое описание: Обход безопасности в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-23918

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

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-01627

17

Краткое описание: Выполнение произвольного кода в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-0767

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-01270

18

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-22809

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-00210

19

Краткое описание: Повышение привилегий в Juniper Networks Session Smart Router

Идентификатор уязвимости: CVE-2023-0461

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Session Smart Router: до 6.2.3-r2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-01200

20

Краткое описание: Выполнение произвольного кода в D-Link DCS-8300LHV2

Идентификатор уязвимости: CVE-2023-51628

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DCS-8300LHv2: 1.06.01

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-15 / 2024-01-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-048/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370

21

Краткое описание: Выполнение произвольного кода в D-Link DCS-8300LHV2

Идентификатор уязвимости: CVE-2023-51626

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DCS-8300LHv2: 1.06.01

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-15 / 2024-01-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-046/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370

Краткое описание: Выполнение произвольного кода в D-Link DCS-8300LHV2

Идентификатор уязвимости: CVE-2023-51625

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

Уязвимый продукт: DCS-8300LHv2: 1.06.01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-15 / 2024-01-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-045/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370

23

Краткое описание: Выполнение произвольного кода в D-Link DCS-8300LHV2

Идентификатор уязвимости: CVE-2023-51624

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DCS-8300LHv2: 1.06.01

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-15 / 2024-01-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-044/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370

24

Краткое описание: Выполнение произвольного кода в D-Link DCS-8300LHV2

Идентификатор уязвимости: CVE-2023-51627

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DCS-8300LHv2: 1.06.01

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-15 / 2024-01-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-047/
- http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370