НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-19.1 | 19 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-20419	Cisco Smart Software Manager On-Prem	Сетевой	OSI	2024-07-18	✓
2	Высокая	BDU:2024-05247	Кейсистемс "Сервис оправдательных документов"	Сетевой	RLF	2024-05-15	✓
3	Высокая	BDU:2024-05246	Кейсистемс "Сервис оправдательных документов"	Сетевой	RLF	2024-05-15	✓
4	Высокая	BDU:2024-05245	Кейсистемс "Управление сервисами СМАРТ/WEB"	Сетевой	RLF	2024-05-15	✓
5	Средняя	BDU:2024-05244	Кейсистемс "Проект-СмартПРО"	Сетевой	ACE	2024-05-15	✓
6	Высокая	BDU:2024-05243	Кейсистемс "Сервис оправдательных документов	Сетевой	RLF	2024-05-15	✓
7	Средняя	BDU:2024-05242	Кейсистемс "Сервис обновлений"	Сетевой	RLF	2024-05-15	✓
8	Средняя	BDU:2024-05241	Кейсистемс "Сервис обновлений"	Сетевой	RLF	2024-05-15	✓
9	Средняя	BDU:2024-05240	Кейсистемс "Сервис обновлений"	Сетевой	RLF	2024-05-15	✓
10	Средняя	BDU:2024-05239	Кейсистемс "Сервис обновлений"	Сетевой	RLF	2024-05-15	✓
11	Высокая	CVE-2024-39551	Junos OS	Сетевой	DoS	2024-07-11	✓
12	Высокая	CVE-2024-39520	Junos OS	Локальный	PE	2024-07-11	✓

13	Высокая	CVE-2024-39555	Junos OS and Junos OS Evolved RPD	Сетевой	DoS	2024-07-15	✓
14	Высокая	CVE-2024-39529	Junos OS	Сетевой	DoS	2024-07-11	✓
15	Высокая	CVE-2024-39540	Junos OS	Сетевой	DoS	2024-07-11	✓
16	Высокая	CVE-2024-39531	Junos OS Evolved PFE	Сетевой	DoS	2024-07-15	✓
17	Высокая	CVE-2024-39542	Junos OS and Junos OS Evolved PFE	Сетевой	DoS	2024-07-15	✓
18	Высокая	CVE-2024-39545	Junos OS	Сетевой	DoS	2024-07-12	✓
19	Высокая	CVE-2024-39549	Junos OS and Junos OS Evolved rpd	Сетевой	DoS	2024-07-15	✓
20	Высокая	CVE-2024-39552	Junos OS and Junos OS Evolved RPD	Сетевой	DoS	2024-07-16	✓
21	Высокая	CVE-2024-23663	FortiExtender	Сетевой	SB	2024-07-09	✓

1

Краткое описание: Получение конфиденциальной информации в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2024-20419

Идентификатор программной ошибки: CWE-620 Смена пароля без подтверждения

Уязвимый продукт: Cisco Smart Software Manager On-Prem: версии 8-202206

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2024-07-18 / 2024-07-18

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy

2

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис оправдательных документов"

Идентификатор уязвимости: BDU:2024-05247

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.].../...//[1.ков.]

Уязвимый продукт: Кейсистемс "Сервис оправдательных документов": версии 3.2.6158, 3.2.6177, 3.2.6241, 3.2.6283, 3.3.6466, 3.3.6666, 3.3.7142, 3.3.7193, 3.3.7206, 3.3.7335, 3.3.7838, 3.3.8011.14961, 3.3.8066.31284, 3.3.8067.16845, 3.3.8241.14945, 3.3.8273.28985, 3.3.8304.28872, 3.3.8307.28596, 3.3.8327.19869, 3.3.8363.26340, 3.3.8388.17215, 3.3.8495.20777, 3.3.8602.22545, 3.3.8602.24861, 3.3.8607.27783, 3.3.8608.16338, 3.3.8609.28136, 3.3.8614.21335, 3.3.8629.31065, 3.3.8636.20149, 3.3.8647.14847, 3.3.8714.14547, 3.3.8717.17569, 3.3.8719.17542, 3.3.8724.32399, 3.3.8732.14684, 3.3.8783.19305

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05247
- https://www.keysystems.ru/update/

3

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис оправдательных документов"

Идентификатор уязвимости: BDU:2024-05246

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.].../...//[1.ков.]

Уязвимый продукт: Кейсистемс "Сервис оправдательных документов": версии 3.3.8160.881, 3.3.8195.554, 3.3.8195.560, 3.3.8195.887, 3.3.8195.894, 3.3.8195.1325, 3.3.8195.1332, 3.3.8202.800, 3.3.8230.686, 3.3.8230.997, 3.3.8241.516, 3.3.8273.965, 3.3.8278.622, 3.3.8280.1284, 3.3.8304.967, 3.3.8307.953, 3.3.8321.537, 3.3.8328.1025, 3.3.8495.698, 6.0.8735.569, 6.0.8745.1046, 6.0.8783.674, 6.0.8783.1047

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05246
- https://www.keysystems.ru/update/

4

Краткое описание: Чтение локальных файлов в Кейсистемс "Управление сервисами CMAPT/WEB"

Идентификатор уязвимости: BDU:2024-05245

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Кейсистемс "Управление сервисами CMAPT/WEB": версии 1.4.2015.26586, 1.4.2015.37517, 1.4.2015.9130, 1.9.2023.44306

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05245
- https://www.keysystems.ru/update/

Краткое описание: Выполнение произвольного кода в Кейсистемс "Проект-СмартПРО"

Идентификатор уязвимости: BDU:2024-05244

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: Кейсистемс "Проект-СмартПРО": версии 20.1.38183.0, 21.33.49550.0, 21.33.50142.0, 21.33.53938.0, 21.33.55158.0, 23.11.56634.0, 23.11.57512.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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: 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05244
- https://www.keysystems.ru/update/

6

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис оправдательных документов

Идентификатор уязвимости: BDU:2024-05243

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.].../...//[1.ков.]

Уязвимый продукт: Кейсистемс "Сервис оправдательных документов": с версии 2.1.11341.006 по 2.2.11342.002 и 2.2.11342.005

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05243
- https://www.keysystems.ru/update/

7

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис обновлений"

Идентификатор уязвимости: BDU:2024-05242

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: Кейсистемс "Сервис обновлений": версии 3.2.6143, 3.2.6191, 3.3.6544, 3.3.8200, 2.2.11340.27671

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-05242
- https://www.keysystems.ru/update/

8

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис обновлений"

Идентификатор уязвимости: BDU:2024-05241

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.].../...//[1.ков.]

Уязвимый продукт: Кейсистемс "Сервис обновлений": версии 3.2.6143, 3.2.6191, 3.3.6544, 3.3.8200, 3.3.8207.18015, 3.3.8279.14186

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://www.keysystems.ru/update/
- https://bdu.fstec.ru/vul/2024-05241

9

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис обновлений"

Идентификатор уязвимости: BDU:2024-05240

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: Кейсистемс "Сервис обновлений": версии 2.2.11340.27671

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://www.keysystems.ru/update/
- https://bdu.fstec.ru/vul/2024-05240

Краткое описание: Чтение локальных файлов в Кейсистемс "Сервис обновлений"

Идентификатор уязвимости: BDU:2024-05239

Идентификатор программной ошибки: CWE-35 Выход за пределы каталога с помощью [1.ков.]../...//[1.ков.]

Уязвимый продукт: Кейсистемс "Сервис обновлений": версии 3.2.6143, 3.2.6191, 3.3.6544, 3.3.8200, 3.3.8207.18015, 3.3.8279.14186, 6.0.8735.611, 6.0.8741.526

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- https://www.keysystems.ru/update/
- https://bdu.fstec.ru/vul/2024-05239

11

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-39551

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

Уязвимый продукт: Juniper Networks Junos OS on SRX Series and MX Series with SPC3 and MS-MPC/MIC

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 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: 2024-07-11 / 2024-07-11

Ссылки на источник:

- https://supportportal.juniper.net/JSA83013

Краткое описание: Повышение привилегий в Junos OS

Идентификатор уязвимости: CVE-2024-39520

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

Уязвимый продукт: Juniper Networks Junos OS Evolved: до версии 22.3R2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

12

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

Оценка CVSSv3: 7.8 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: 2024-07-11 / 2024-07-11

Ссылки на источник:

- https://supportportal.juniper.net/JSA82975

Краткое описание: Отказ в обслуживании в Junos OS and Junos OS Evolved RPD

Идентификатор уязвимости: CVE-2024-39555

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Junos OS Evolved: 21.4R1-EVO - 23.2R2-EVO
Juniper Junos OS: 21.4R1 - 23.4R1-S1

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

Способ эксплуатации: Отправки специально сформированного eBGP-трафика

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-a-specific-malformed-BGP-update-causes-the-session-to-reset-CVE-2024-39555

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-39529

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

Уязвимый продукт: Juniper Networks Junos OS on SRX Series

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-11 / 2024-07-11

Ссылки на источник:

- https://supportportal.juniper.net/JSA82988

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-39540

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

Уязвимый продукт: Juniper Networks Junos OS: с версии 21.2R3-S5 по 21.2R3-S6.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-07-11 / 2024-07-11

Ссылки на источник:

- https://supportportal.juniper.net/JSA83000

16

Краткое описание: Отказ в обслуживании в Junos OS Evolved PFE

Идентификатор уязвимости: CVE-2024-39531

Идентификатор программной ошибки: CWE-229 Некорректная обработка значений

Уязвимый продукт: Junos OS Evolved: с версии 21.4R1-EVO по 23.2R1-S2-EVO

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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-Evolved-ACX7000-Series-Protocol-specific-DDoS-configuration-affects-other-protocols-CVE-2024-39531

Краткое описание: Отказ в обслуживании в Junos OS and Junos OS Evolved PFE

Идентификатор уязвимости: CVE-2024-39542

Идентификатор программной ошибки: CWE-1286 Некорректная проверка правильности синтаксиса входных данных

Уязвимый продукт: Junos OS Evolved и Juniper Junos OS:
Junos OS Evolved: с версии 21.2-EVO по 22.2-EVO
Juniper Junos OS: с версии 21.2R1 по 22.3R1-S2

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-malformed-CFM-packet-or-specific-transit-traffic-leads-to-FPC-crash-CVE-2024-39542

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-39545

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

Уязвимый продукт: Juniper Junos OS: с версии 21.2R1 по 23.2R1-S2

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2024-07-12 / 2024-07-12

Ссылки на источник:

- http://supportportal.juniper.net/JSA83007

Краткое описание: Отказ в обслуживании в Junos OS and Junos OS Evolved rpd

Идентификатор уязвимости: CVE-2024-39549

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Junos OS и Junos OS Evolved:
Juniper Junos OS: с версии 21.2R1 по 23.4R1-S1
Junos OS Evolved: с версии 21.2-EVO по 23.2R2-EVO

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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-Receipt-of-malformed-BGP-path-attributes-leads-to-a-memory-leak-CVE-2024-39549

Краткое описание: Отказ в обслуживании в Junos OS and Junos OS Evolved RPD

Идентификатор уязвимости: CVE-2024-39552

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: Junos OS и Junos OS Evolved:
Junos OS Evolved: с версии 21.2-EVO по 23.2R1-S2-EVO
Juniper Junos OS: с версии 20.4R1 по 23.4R1-S2

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

20

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

Оценка CVSSv3: 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: 2024-07-16 / 2024-07-16

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Malformed-BGP-UPDATE-causes-RPD-crash-CVE-2024-39552

Краткое описание: Обход безопасности в FortiExtender

Идентификатор уязвимости: CVE-2024-23663

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: FortiExtender: с версии 7.0.0 по 7.4.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Обход безопасности

21 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-459