

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-29.1 | 29 ноября 2023 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-6345	Google Chrome	Сетевой	ACE	2023-11-28	✓
2	Критическая	CVE-2023-6351	Google Chrome	Сетевой	ACE	2023-11-28	✓
3	Критическая	CVE-2023-6350	Google Chrome	Сетевой	ACE	2023-11-28	✓
4	Критическая	CVE-2023-6346	Google Chrome	Сетевой	ACE	2023-11-28	✓
5	Критическая	CVE-2023-6347	Google Chrome	Сетевой	ACE	2023-11-28	✓
6	Высокая	CVE-2023-6348	Google Chrome	Сетевой	ACE	2023-11-28	✓
7	Высокая	CVE-2022-46337	Apache Derby	Сетевой	SB	2023-11-28	✓
8	Критическая	CVE-2023-6329	Control ID iDSecure	Сетевой	SB	2023-11-28	✗
9	Высокая	CVE-2023-31275	WPS Office	Сетевой	ACE	2023-11-28	✗
10	Высокая	CVE-2022-25647	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
11	Высокая	CVE-2021-37714	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
12	Высокая	CVE-2022-42003	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
13	Высокая	CVE-2021-46877	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓

14	Высокая	CVE-2020-36518	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
15	Высокая	CVE-2023-44487	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
16	Высокая	CVE-2023-42794	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
17	Высокая	CVE-2023-0217	Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG	Сетевой	DoS	2023-11-22	✓
18	Высокая	CVE-2023-0401	Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG	Сетевой	DoS	2023-11-22	✓
19	Критическая	CVE-2023-45797	Dream Security MagicLine4NX	Сетевой	ACE	2023-11-27	✓
20	Высокая	CVE-2022-42004	Jira Software и Data Center	Сетевой	DoS	2023-11-22	✓
21	Высокая	CVE-2023-48228	authentik	Сетевой	SB	2023-11-24	✓
22	Высокая	CVE-2023-40152	Tellus Lite V-Simulator	Локальный	ACE	2023-11-22	✓
23	Высокая	CVE-2023-40718	Fortinet IPS Engine	Сетевой	SB	2023-10-10	✓
24	Критическая	CVE-2023-47678	ASUS RT-AC87U	Сетевой	WLF	2023-11-27	✗
25	Критическая	CVE-2023-20048	Cisco Firepower Management Center	Сетевой	ACE	2023-11-02	✓
26	Критическая	CVE-2023-36553	FortiSIEM	Сетевой	ACE	2023-11-17	✓
27	Высокая	CVE-2023-20175	Cisco Identity Services Engine (ISE)	Локальный	ACE	2023-11-03	✓
28	Высокая	CVE-2023-20063	Cisco FTD и FMC	Локальный	ACE	2023-11-02	✓

29	Высокая	CVE-2023-20220	Cisco Firepower Management Center	Сетевой	ACE	2023-11-02	✓
30	Высокая	CVE-2023-20219	Cisco Firepower Management Center	Сетевой	ACE	2023-11-02	✓

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6345

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6351

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

2 **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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6350

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

3 **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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6346

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

- 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: 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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6347

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6348

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смещение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.160

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Краткое описание: Обход безопасности в Apache Derby

Идентификатор уязвимости: CVE-2022-46337

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: Apache Derby: 10.1.1 - 10.16.1.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-28 / 2023-11-28

Ссылки на источник:

- <http://lists.apache.org/thread/q23kvtoohgzwybpxpwozmvk17rp0td3>

Краткое описание: Обход безопасности в Control ID iDSecure

Идентификатор уязвимости: CVE-2023-6329

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Control ID iDSecure: 4.7.32.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

8 **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: 2023-11-28 / 2023-11-28

Ссылки на источник:

- <http://tenable.com/security/research/tra-2023-36>

Краткое описание: Выполнение произвольного кода в WPS Office

Идентификатор уязвимости: CVE-2023-31275

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: WPS Office: 11.2.0.11537

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

9 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:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-28 / 2023-11-28

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1748

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2022-25647

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25412>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2021-37714

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (защипливание)

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой
1 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25410>
- <https://bdu.fstec.ru/vul/2023-05361>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2022-42003

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой
2 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25408>
- <https://bdu.fstec.ru/vul/2023-05618>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2021-46877

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
3

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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25407>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2020-36518

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25406>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
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: 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25398>
- <https://bdu.fstec.ru/vul/2023-06559>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2023-42794

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

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
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: 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25400>
- <https://bdu.fstec.ru/vul/2023-06729>

Краткое описание: Отказ в обслуживании в Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG

Идентификатор уязвимости: CVE-2023-0217

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG: до версии 4.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
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: 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-699386.txt>
- <http://www.openssl.org/news/secadv/20230207.txt>

Краткое описание: Отказ в обслуживании в Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG

Идентификатор уязвимости: CVE-2023-0401

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Siemens SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG: до версии 4.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

1
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: 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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://cert-portal.siemens.com/productcert/txt/ssa-699386.txt>
- <http://www.openssl.org/news/secadv/20230207.txt>

Краткое описание: Выполнение произвольного кода в Dream Security MagicLine4NX

Идентификатор уязвимости: CVE-2023-45797

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

Уязвимый продукт: Dream Security MagicLine4NX: 1.0.0.1 - 1.0.0.26

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

1
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: 9.8 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: 2023-11-27 / 2023-11-27

Ссылки на источник:

- <http://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&nttId=71023&menuNo=205020>
- <http://s3.documentcloud.org/documents/24174869/rok-uk-joint-cyber-security-advisoryeng.pdf>

Краткое описание: Отказ в обслуживании в Jira Software и Data Center

Идентификатор уязвимости: CVE-2022-42004

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

Уязвимый продукт: Jira Software и Data Center: 8.0.0 - 9.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

2
0

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: 2023-11-22 / 2023-11-22

Ссылки на источник:

- <http://jira.atlassian.com/browse/JSWSERVER-25409>
- <https://bdu.fstec.ru/vul/2023-05617>

Краткое описание: Обход безопасности в authentik

Идентификатор уязвимости: CVE-2023-48228

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: authentik: 2023.8.0 - 2023.10.3

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2023-11-24 / 2023-11-24

Ссылки на источник:

- <http://github.com/goauthentik/authentik/security/advisories/GHSA-fm34-v8xq-f2c3>
- <http://github.com/goauthentik/authentik/pull/7666>
- <http://github.com/goauthentik/authentik/pull/7668>
- <http://github.com/goauthentik/authentik/pull/7669>
- <http://github.com/goauthentik/authentik/commit/3af77ab3821fe9c7df8055ba5eade3d1ecea03a6>
- <http://github.com/goauthentik/authentik/commit/6b9afed21f7c39f171a4a445654cfe415bba37d5>
- <http://github.com/goauthentik/authentik/commit/b88e39411c12e3f9e04125a7887f12354f760a14>
- <http://github.com/goauthentik/authentik/blob/dd4e9030b4e667d3720be2feda24c08972602274/authentik/providers/oauth2/views/token.py#L225>
- <http://github.com/goauthentik/authentik/releases/tag/version%2F2023.10.4>
- <http://github.com/goauthentik/authentik/releases/tag/version%2F2023.8.5>

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

Идентификатор уязвимости: CVE-2023-40152

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

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.

2
2

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
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1735/>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1729/>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1725/>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1724/>

Краткое описание: Обход безопасности в Fortinet IPS Engine

Идентификатор уязвимости: CVE-2023-40718

Идентификатор программной ошибки: CWE-436 Конфликт интерпретации

Уязвимый продукт: Fortinet IPS Engine: версии до 7.3.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: обход безопасности

2
3

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: 2023-10-10 / 2023-11-06

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2023-06717>

Краткое описание: Запись локальных файлов в ASUS RT-AC87U

Идентификатор уязвимости: CVE-2023-47678

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: ASUS RT-AC87U: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: запись локальных файлов

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

Оценка CVSSv3: 9.1 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: 2023-11-27 / 2023-11-27

Ссылки на источник:

- <http://www.asus.com/support/>
- <http://www.asus.com/event/network/EOL-product/>
- <http://jvn.jp/en/vu/JVNVU96079387/>

Краткое описание: Выполнение произвольного кода в Cisco Firepower Management Center

Идентификатор уязвимости: CVE-2023-20048

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

Уязвимый продукт: Cisco Firepower Management Center: 6.2.3 - 7.4.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

2
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: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-02 / 2023-11-02

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-29MP49hN>
- <https://bdu.fstec.ru/vul/2023-07476>

Краткое описание: Выполнение произвольного кода в FortiSIEM

Идентификатор уязвимости: CVE-2023-36553

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

Уязвимый продукт: FortiSIEM: 4.7.2 - 5.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

2
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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-17 / 2023-11-17

Ссылки на источник:

- <http://fortiguard.com/psirt/FG-IR-23-135>
- <https://bdu.fstec.ru/vul/2023-07936>

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2023-20175

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

Уязвимый продукт: Cisco Identity Services Engine (ISE): 3.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

2
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: 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-03 / 2023-11-03

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-QeXegrCw>

Краткое описание: Выполнение произвольного кода в Cisco FTD и FMC

Идентификатор уязвимости: CVE-2023-20063

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

Уязвимый продукт: Cisco FTD и FMC:
Firepowe Threat Defense (FTD): 6.6.0 - 7.2.0
Firepowe Management Center(FMC): 6.6.0 - 7.2.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-02 / 2023-11-02

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-fmc-code-inj-wSHrgz8L>

Краткое описание: Выполнение произвольного кода в Cisco Firepower Management Center

Идентификатор уязвимости: CVE-2023-20220

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

Уязвимый продукт: Cisco Firepower Management Center: 6.2.0 - 7.1.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

2
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: 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: 2023-11-02 / 2023-11-02

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmdinj-bTEgufOX>

Краткое описание: Выполнение произвольного кода в Cisco Firepower Management Center

Идентификатор уязвимости: CVE-2023-20219

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

Уязвимый продукт: Cisco Firepower Management Center: 6.7.0 - 7.4.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

3
0

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: 2023-11-02 / 2023-11-02

Ссылки на источник:

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmdinj-bTEgufOX>