НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-03-18.1 | 18 марта 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-22640	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-18	✗
2	Высокая	CVE-2022-42476	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Локальный	PE	2024-03-18	✗
3	Высокая	CVE-2022-41334	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	XSS\CSS	2024-03-18	✗
4	Высокая	CVE-2022-41327	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Локальный	OSI	2024-03-18	✗
5	Критическая	CVE-2023-33308	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-18	✗
6	Критическая	CVE-2023-27997	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-18	✗
7	Критическая	CVE-2023-25610	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-18	✗
8	Высокая	CVE-2022-41330	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	XSS\CSS	2024-03-18	✗
9	Высокая	CVE-2023-41841	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	PE	2024-03-18	✗
10	Высокая	CVE-2023-40718	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	SB	2024-03-18	✗

11	Высокая	CVE-2023-29183	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	XSS\CSS	2024-03-18	✗
12	Высокая	CVE-2023-29181	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-18	✗
13	Высокая	CVE-2023-29180	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	DoS	2024-03-18	✗
14	Высокая	CVE-2024-22045	Siemens SINEMA Remote Connect Client	Сетевой	OSI	2024-03-13	✓
15	Критическая	CVE-2024-1917	Mitsubishi Electric MELSEC-Q/L Series	Сетевой	ACE	2024-03-15	✗
16	Критическая	CVE-2024-1916	Mitsubishi Electric MELSEC-Q/L Series	Сетевой	ACE	2024-03-15	✗
17	Критическая	CVE-2024-1915	Mitsubishi Electric MELSEC-Q/L Series	Сетевой	ACE	2024-03-15	✗
18	Критическая	CVE-2024-0803	Mitsubishi Electric MELSEC-Q/L Series	Сетевой	ACE	2024-03-15	✗
19	Критическая	CVE-2024-0802	Mitsubishi Electric MELSEC-Q/L Series	Сетевой	ACE	2024-03-15	✗
20	Высокая	CVE-2023-33850	Juniper Secure Analytics (JSA)	Сетевой	OSI	2024-03-15	✓
21	Критическая	CVE-2022-46337	Juniper Secure Analytics (JSA)	Сетевой	SB	2024-03-15	✓
22	Высокая	CVE-2022-34169	Juniper Secure Analytics (JSA)	Сетевой	ACE	2024-03-15	✓
23	Критическая	CVE-2024-27096	GLPI	Сетевой	ACE	2024-03-14	✓
24	Высокая	CVE-2023-36554	Fortinet FortiManager	Сетевой	ACE	2024-03-14	✓

25	Высокая	CVE-2023-44487	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	DoS	2024-03-13	✗
26	Высокая	CVE-2023-44250	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	PE	2024-03-13	✗
27	Критическая	CVE-2023-38545	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-13	✗
28	Критическая	CVE-2024-23113	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-13	✗
29	Критическая	CVE-2024-21762	Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2024-03-13	✗
30	Высокая	CVE-2023-42790	FortiOS and FortiProxy captive portal	Сетевой	ACE	2024-03-13	✓
31	Критическая	CVE-2023-42789	FortiOS and FortiProxy captive portal	Сетевой	ACE	2024-03-13	✓
32	Высокая	CVE-2023-49125	Siemens Solid Edge	Локальный	OSI	2024-03-13	✓
33	Высокая	CVE-2024-2229	Schneider Electric EcoStruxure Power Design	Сетевой	ACE	2024-03-13	✗
34	Высокая	CVE-2024-2400	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-03-13	✓
35	Критическая	CVE-2024-22039	Siemens Sinteso EN and Cerberus PRO EN Fire Protection Systems	Сетевой	ACE	2024-03-13	✓
36	Высокая	CVE-2024-23612	NI LabVIEW	Локальный	ACE	2024-03-13	✓
37	Высокая	CVE-2024-23611	NI LabVIEW	Локальный	ACE	2024-03-13	✓

38	Высокая	CVE-2024-23610	NI LabVIEW	Локальный	ACE	2024-03-13	✓
39	Высокая	CVE-2024-23608	NI LabVIEW	Локальный	ACE	2024-03-13	✓
40	Высокая	CVE-2024-23609	NI LabVIEW	Локальный	ACE	2024-03-13	✓

1

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-22640

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-02603

2

Краткое описание: Повышение привилегий в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2022-42476

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-01331

3

Краткое описание: Межсайтовый скриптинг в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2022-41334

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt

4

Краткое описание: Получение конфиденциальной информации в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2022-41327

Идентификатор программной ошибки: CWE-319 Передача важных данных в незашифрованном виде

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-03357

5

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-33308

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: RUGGEDCOM APE1808: все версии

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-03690

6

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-27997

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-03157

7

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-25610

Идентификатор программной ошибки: CWE-124 Запись данных в область перед началом буфера

Уязвимый продукт: RUGGEDCOM APE1808: все версии

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/E:P/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-01148

8

Краткое описание: Межсайтовый скриптинг в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2022-41330

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: межсайтовый скриптинг

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt

9

Краткое описание: Повышение привилегий в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-41841

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-06706

Краткое описание: Обход безопасности в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-40718

Идентификатор программной ошибки: CWE-436 Конфликт интерпретации

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: обход безопасности

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

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-06717

Краткое описание: Межсайтовый скриптинг в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-29183

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: межсайтовый скриптинг

11

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

Оценка CVSSv3: 8.0 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-05688

12

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-29181

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-03509

13

Краткое описание: Отказ в обслуживании в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-29180

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-03-18 / 2024-03-18

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-366067.txt
- https://bdu.fstec.ru/vul/2023-03351

14

Краткое описание: Получение конфиденциальной информации в Siemens SINEMA Remote Connect Client

Идентификатор уязвимости: CVE-2024-22045

Идентификатор программной ошибки: CWE-538 Разглашение информации, связанное с файлами и каталогами

Уязвимый продукт: SINEMA Remote Connect Client: до 3.1 SP1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-653855.html

15

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC-Q/L Series

Идентификатор уязвимости: CVE-2024-1917

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

Уязвимый продукт: MELSEC-Q Q03UDECPU: все версии
Q04UDEHCPU: все версии
MELSEC iQ-Q 06 UDEHCPU: все версии
MELSEC iQ-Q 10 UDEHCPU: все версии
MELSEC iQ-Q 13 UDEHCPU: все версии
MELSEC iQ-Q 20 UDEHCPU: все версии
MELSEC iQ-Q 26 UDEHCPU: все версии
MELSEC iQ-Q 50 UDEHCPU: все версии
MELSEC iQ-Q 100 UDEHCPU: все версии
MELSEC iQ-Q 03 UDVCPU: все версии
MELSEC iQ-Q 04 UDVCPU: все версии
MELSEC iQ-Q 06 UDVCPU: все версии
MELSEC iQ-Q 13 UDVCPU: все версии
MELSEC iQ-Q 26 UDVCPU: все версии
MELSEC iQ-Q 04 UDPVCPU: все версии
MELSEC iQ-Q 06 UDPVCPU: все версии
MELSEC iQ-Q 13 UDPVCPU: все версии
MELSEC iQ-Q 26 UDPVCPU: все версии
MELSEC L Series L02CPU(-P): все версии
MELSEC L Series L06CPU(-P): все версии
MELSEC L Series L26CPU(-P): все версии
MELSEC L Series L26CPU-(P)BT: все версии

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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf

16

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC-Q/L Series

Идентификатор уязвимости: CVE-2024-1916

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

Уязвимый продукт: MELSEC-Q Q03UDECPU: все версии
Q04UDEHCPU: все версии
MELSEC iQ-Q 06 UDEHCPU: все версии
MELSEC iQ-Q 10 UDEHCPU: все версии
MELSEC iQ-Q 13 UDEHCPU: все версии
MELSEC iQ-Q 20 UDEHCPU: все версии
MELSEC iQ-Q 26 UDEHCPU: все версии
MELSEC iQ-Q 50 UDEHCPU: все версии
MELSEC iQ-Q 100 UDEHCPU: все версии
MELSEC iQ-Q 03 UDVCPU: все версии
MELSEC iQ-Q 04 UDVCPU: все версии
MELSEC iQ-Q 06 UDVCPU: все версии
MELSEC iQ-Q 13 UDVCPU: все версии
MELSEC iQ-Q 26 UDVCPU: все версии
MELSEC iQ-Q 04 UDPVCPU: все версии
MELSEC iQ-Q 06 UDPVCPU: все версии
MELSEC iQ-Q 13 UDPVCPU: все версии
MELSEC iQ-Q 26 UDPVCPU: все версии
MELSEC L Series L02CPU(-P): все версии
MELSEC L Series L06CPU(-P): все версии
MELSEC L Series L26CPU(-P): все версии
MELSEC L Series L26CPU-(P)BT: все версии

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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf

17

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC-Q/L Series

Идентификатор уязвимости: CVE-2024-1915

Идентификатор программной ошибки: CWE-468 Некорректное масштабирование указателей

Уязвимый продукт: MELSEC-Q Q03UDECPU: все версии
Q04UDEHCPU: все версии
MELSEC iQ-Q 06 UDEHCPU: все версии
MELSEC iQ-Q 10 UDEHCPU: все версии
MELSEC iQ-Q 13 UDEHCPU: все версии
MELSEC iQ-Q 20 UDEHCPU: все версии
MELSEC iQ-Q 26 UDEHCPU: все версии
MELSEC iQ-Q 50 UDEHCPU: все версии
MELSEC iQ-Q 100 UDEHCPU: все версии
MELSEC iQ-Q 03 UDVCPU: все версии
MELSEC iQ-Q 04 UDVCPU: все версии
MELSEC iQ-Q 06 UDVCPU: все версии
MELSEC iQ-Q 13 UDVCPU: все версии
MELSEC iQ-Q 26 UDVCPU: все версии
MELSEC iQ-Q 04 UDPVCPU: все версии
MELSEC iQ-Q 06 UDPVCPU: все версии
MELSEC iQ-Q 13 UDPVCPU: все версии
MELSEC iQ-Q 26 UDPVCPU: все версии
MELSEC L Series L02CPU(-P): все версии
MELSEC L Series L06CPU(-P): все версии
MELSEC L Series L26CPU(-P): все версии
MELSEC L Series L26CPU-(P)BT: все версии

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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf

18

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC-Q/L Series

Идентификатор уязвимости: CVE-2024-0803

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

Уязвимый продукт: MELSEC-Q Q03UDECPU: все версии
Q04UDEHCPU: все версии
MELSEC iQ-Q 06 UDEHCPU: все версии
MELSEC iQ-Q 10 UDEHCPU: все версии
MELSEC iQ-Q 13 UDEHCPU: все версии
MELSEC iQ-Q 20 UDEHCPU: все версии
MELSEC iQ-Q 26 UDEHCPU: все версии
MELSEC iQ-Q 50 UDEHCPU: все версии
MELSEC iQ-Q 100 UDEHCPU: все версии
MELSEC iQ-Q 03 UDVCPU: все версии
MELSEC iQ-Q 04 UDVCPU: все версии
MELSEC iQ-Q 06 UDVCPU: все версии
MELSEC iQ-Q 13 UDVCPU: все версии
MELSEC iQ-Q 26 UDVCPU: все версии
MELSEC iQ-Q 04 UDPVCPU: все версии
MELSEC iQ-Q 06 UDPVCPU: все версии
MELSEC iQ-Q 13 UDPVCPU: все версии
MELSEC iQ-Q 26 UDPVCPU: все версии
MELSEC L Series L02CPU(-P): все версии
MELSEC L Series L06CPU(-P): все версии
MELSEC L Series L26CPU(-P): все версии
MELSEC L Series L26CPU-(P)BT: все версии

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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf

19

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric MELSEC-Q/L Series

Идентификатор уязвимости: CVE-2024-0802

Идентификатор программной ошибки: CWE-468 Некорректное масштабирование указателей

Уязвимый продукт: MELSEC-Q Q03UDECPU: все версии
Q04UDEHCPU: все версии
MELSEC iQ-Q 06 UDEHCPU: все версии
MELSEC iQ-Q 10 UDEHCPU: все версии
MELSEC iQ-Q 13 UDEHCPU: все версии
MELSEC iQ-Q 20 UDEHCPU: все версии
MELSEC iQ-Q 26 UDEHCPU: все версии
MELSEC iQ-Q 50 UDEHCPU: все версии
MELSEC iQ-Q 100 UDEHCPU: все версии
MELSEC iQ-Q 03 UDVCPU: все версии
MELSEC iQ-Q 04 UDVCPU: все версии
MELSEC iQ-Q 06 UDVCPU: все версии
MELSEC iQ-Q 13 UDVCPU: все версии
MELSEC iQ-Q 26 UDVCPU: все версии
MELSEC iQ-Q 04 UDPVCPU: все версии
MELSEC iQ-Q 06 UDPVCPU: все версии
MELSEC iQ-Q 13 UDPVCPU: все версии
MELSEC iQ-Q 26 UDPVCPU: все версии
MELSEC L Series L02CPU(-P): все версии
MELSEC L Series L06CPU(-P): все версии
MELSEC L Series L26CPU(-P): все версии
MELSEC L Series L26CPU-(P)BT: все версии

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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-024_en.pdf
- https://bdu.fstec.ru/vul/2024-02053

20

Краткое описание: Получение конфиденциальной информации в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-33850

Идентификатор программной ошибки: CWE-203 Наблюдаемые различия в поведении в ответ на некорректный ввод

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF05

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP7-IF06

21

Краткое описание: Обход безопасности в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2022-46337

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

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF05

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного запроса.

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: 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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP7-IF06
- https://bdu.fstec.ru/vul/2024-00180

22

Краткое описание: Выполнение произвольного кода в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2022-34169

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF05

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: 7.5 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: 2024-03-15 / 2024-03-15

Ссылки на источник:

- http://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP7-IF06
- https://bdu.fstec.ru/vul/2022-04788

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2024-27096

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: GLPI: 10.0.0 - 10.0.12

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

23

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-14 / 2024-03-14

Ссылки на источник:

- http://github.com/glpi-project/glpi/releases/tag/10.0.13
- http://glpi-project.org/glpi-release-10-0-13/

24

Краткое описание: Выполнение произвольного кода в Fortinet FortiManager

Идентификатор уязвимости: CVE-2023-36554

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: FortiManager: 6.2.0 - 7.4.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход ограничений безопасности

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: 8.1 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: 2024-03-14 / 2024-03-14

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-103
- https://bdu.fstec.ru/vul/2024-02018

Краткое описание: Отказ в обслуживании в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-832273.txt
- https://bdu.fstec.ru/vul/2023-06559

Краткое описание: Повышение привилегий в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-44250

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: повышение привилегий

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

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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-832273.txt
- https://bdu.fstec.ru/vul/2024-00117

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-38545

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-832273.txt
- https://bdu.fstec.ru/vul/2023-06576

28

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2024-23113

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

Уязвимый продукт: RUGGEDCOM APE1808: все версии

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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-832273.txt
- https://bdu.fstec.ru/vul/2024-01122

Краткое описание: Выполнение произвольного кода в Fortigate NGFW on Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2024-21762

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: RUGGEDCOM APE1808: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-832273.txt
- https://bdu.fstec.ru/vul/2024-01125

Краткое описание: Выполнение произвольного кода в FortiOS and FortiProxy captive portal

Идентификатор уязвимости: CVE-2023-42790

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: FortiOS: 6.2.12 - 7.4.1
FortiProxy: 2.0.10 - 7.4.0

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-327
- https://bdu.fstec.ru/vul/2024-02011

Краткое описание: Выполнение произвольного кода в FortiOS and FortiProxy captive portal

Идентификатор уязвимости: CVE-2023-42789

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FortiOS: 6.2.0 - 7.4.1
FortiProxy: 2.0.0 - 7.4.0

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

31

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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-328
- https://bdu.fstec.ru/vul/2024-01949

Краткое описание: Получение конфиденциальной информации в Siemens Solid Edge

Идентификатор уязвимости: CVE-2023-49125

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Solid Edge: до 223.0.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: получение конфиденциальной информации

32 **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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-382651.txt

Краткое описание: Выполнение произвольного кода в Schneider Electric EcoStruxure Power Design

Идентификатор уязвимости: CVE-2024-2229

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: EcoStruxure Power Design - Ecodial NL: все версии
EcoStruxure Power Design - Ecodial INT: все версии
EcoStruxure Power Design - Ecodial FR: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

33 **Последствия эксплуатации:** выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-072-01

34

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-2400

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 120.0.6099.62 - 122.0.6261.112
Microsoft Edge: 79.0.309.71 - 122.0.2365.80

Категория уязвимого продукта: Прикладное программное обеспечение

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

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_12.html
- http://crbug.com/327696052
- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-26163

35

Краткое описание: Выполнение произвольного кода в Siemens Sinteso EN and Cerberus PRO EN Fire Protection Systems

Идентификатор уязвимости: CVE-2024-22039

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

Уязвимый продукт: Cerberus PRO EN Engineering Tool: до IP8
Cerberus PRO EN Fire Panel FC72x: до IP8
Cerberus PRO EN X200 Cloud Distribution: до 4.0.5016
Cerberus PRO EN X300 Cloud Distribution: до 4.2.5015
Sinteso FS20 EN Engineering Tool: до MP8
Sinteso FS20 EN Fire Panel FC20: до MP8
Sinteso FS20 EN X200 Cloud Distribution: до 4.0.5016
Sinteso FS20 EN X300 Cloud Distribution: до 4.2.5015
Sinteso Mobile: до 3.0.0

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: 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: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-225840.html
- https://bdu.fstec.ru/vul/2024-01948

36

Краткое описание: Выполнение произвольного кода в NI LabVIEW

Идентификатор уязвимости: CVE-2024-23612

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LabVIEW: 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/improper-error-handling-issues-in-labview.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-289/

37

Краткое описание: Выполнение произвольного кода в NI LabVIEW

Идентификатор уязвимости: CVE-2024-23611

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LabVIEW: 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/out-of-bounds-write-due-to-missing-bounds-check-in-labview.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-288/

38

Краткое описание: Выполнение произвольного кода в NI LabVIEW

Идентификатор уязвимости: CVE-2024-23610

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LabVIEW: 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/out-of-bounds-write-due-to-missing-bounds-check-in-labview.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-287/

39

Краткое описание: Выполнение произвольного кода в NI LabVIEW

Идентификатор уязвимости: CVE-2024-23608

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LabVIEW: 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/out-of-bounds-write-due-to-missing-bounds-check-in-labview.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-286/

40

Краткое описание: Выполнение произвольного кода в NI LabVIEW

Идентификатор уязвимости: CVE-2024-23609

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LabVIEW: 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-13 / 2024-03-13

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/improper-error-handling-issues-in-labview.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-290/
- http://www.zerodayinitiative.com/advisories/ZDI-24-285/