НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-20.1 | 20 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-34991	Fortinet FortiWLM	Сетевой	ACE	2023-11-20	✓
2	Высокая	CVE-2023-42783	Fortinet FortiWLM	Сетевой	RLF	2023-11-20	✓
3	Высокая	CVE-2023-6063	WP Fastest Cache	Сетевой	ACE	2023-11-16	✓
4	Критическая	CVE-2020-25020	Siemens COMOS	Сетевой	ACE	2023-11-16	✓
5	Высокая	CVE-2022-23095	Siemens COMOS	Локальный	ACE	2023-11-16	✓
6	Высокая	CVE-2022-28807	Siemens COMOS	Локальный	ACE	2023-11-16	✓
7	Высокая	CVE-2022-28808	Siemens COMOS	Локальный	ACE	2023-11-16	✓
8	Высокая	CVE-2022-28809	Siemens COMOS	Локальный	ACE	2023-11-16	✓
9	Высокая	CVE-2023-0933	Siemens COMOS	Сетевой	DoS	2023-11-16	✓
10	Высокая	CVE-2023-1530	Siemens COMOS	Сетевой	ACE	2023-11-16	✓
11	Высокая	CVE-2023-2932	Siemens COMOS	Сетевой	ACE	2023-11-16	✓
12	Высокая	CVE-2023-22669	Siemens COMOS	Локальный	ACE	2023-11-16	✓
13	Высокая	CVE-2023-22670	Siemens COMOS	Локальный	ACE	2023-11-16	✓

14	Критическая	CVE-2023-43504	Siemens COMOS	Сетевой	ACE	2023-11-16	✓
15	Высокая	CVE-2023-2931	Siemens COMOS	Сетевой	ACE	2023-11-16	✓
16	Критическая	CVE-2023-3935	Siemens Desigo CC	Сетевой	ACE	2023-11-16	✗
17	Высокая	CVE-2023-38076	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
18	Высокая	CVE-2023-38075	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
19	Высокая	CVE-2023-38074	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
20	Высокая	CVE-2023-38073	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
21	Высокая	CVE-2023-38072	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
22	Высокая	CVE-2023-38071	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
23	Высокая	CVE-2023-38070	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-11-16	✓
24	Критическая	CVE-2022-37434	Siemens SINEC PNI	Сетевой	ACE	2023-11-16	✓
25	Высокая	CVE-2022-41032	Siemens SINEC PNI	Локальный	PE	2023-11-16	✓
26	Высокая	CVE-2023-21808	Siemens SINEC PNI	Локальный	ACE	2023-11-16	✓
27	Высокая	CVE-2023-24895	Siemens SINEC PNI	Локальный	ACE	2023-11-16	✓
28	Высокая	CVE-2023-24897	Siemens SINEC PNI	Локальный	ACE	2023-11-16	✓

29	Высокая	CVE-2023-28260	Siemens SINEC PNI	Локальный	ACE	2023-11-16	✓
30	Высокая	CVE-2023-29331	Siemens SINEC PNI	Сетевой	DoS	2023-11-16	✓
31	Высокая	CVE-2023-24936	Siemens SINEC PNI	Сетевой	PE	2023-11-16	✓
32	Высокая	CVE-2023-35788	Siemens SIMATIC MV500	Локальный	ACE	2023-11-16	✓
33	Критическая	CVE-2022-23219	Siemens SIMATIC MV500	Сетевой	ACE	2023-11-16	✓
34	Критическая	CVE-2022-23218	Siemens SIMATIC MV500	Сетевой	ACE	2023-11-16	✓
35	Высокая	CVE-2023-29245	Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2023-11-16	✓
36	Высокая	CVE-2023-32649	Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices	Сетевой	DoS	2023-11-16	✓
37	Высокая	CVE-2023-2567	Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices	Сетевой	ACE	2023-11-16	✓
38	Высокая	None	Wireshark	Локальный	ACE	2023-11-16	✓
39	Высокая	CVE-2023-44436	Kofax Power PDF Advanced	Локальный	ACE	2023-11-15	✓
40	Высокая	CVE-2023-44435	Kofax Power PDF Advanced	Локальный	ACE	2023-11-15	✓
41	Высокая	CVE-2023-44432	Kofax Power PDF Advanced	Локальный	ACE	2023-11-15	✓

1

Краткое описание: Выполнение произвольного кода в Fortinet FortiWLM

Идентификатор уязвимости: CVE-2023-34991

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

Уязвимый продукт: Fortinet FortiWLM: 8.2.2 - 8.6.4

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-142
- https://bdu.fstec.ru/vul/2023-07937

2

Краткое описание: Чтение локальных файлов в Fortinet FortiWLM

Идентификатор уязвимости: CVE-2023-42783

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

Уязвимый продукт: Fortinet FortiWLM: 7.0.0 - 8.6.6

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 7.5 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: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-143

3

Краткое описание: Выполнение произвольного кода в WP Fastest Cache

Идентификатор уязвимости: CVE-2023-6063

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

Уязвимый продукт: WP Fastest Cache: 0.8.3.1 - 1.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://wpscan.com/blog/unauthenticated-sql-injection-vulnerability-addressed-in-wp-fastest-cache-1-2-2/
- https://bdu.fstec.ru/vul/2023-07903

4

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2020-25020

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2021-00923

5

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2022-23095

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07888

6

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2022-28807

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2022-04717

7

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2022-28808

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2022-04716

8

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2022-28809

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2022-04715

9

Краткое описание: Отказ в обслуживании в Siemens COMOS

Идентификатор уязвимости: CVE-2023-0933

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-00961

10

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-1530

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens COMOS: до 10.4.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-01617

11

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-2932

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens COMOS: до 10.4.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07645

12

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-22669

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07504

13

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-22670

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07578

14

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-43504

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

Уязвимый продукт: Siemens COMOS: до 10.4.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.6 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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07890

15

Краткое описание: Выполнение произвольного кода в Siemens COMOS

Идентификатор уязвимости: CVE-2023-2931

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens COMOS: до 10.4.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-137900.txt
- https://bdu.fstec.ru/vul/2023-07644

16

Краткое описание: Выполнение произвольного кода в Siemens Desigo CC

Идентификатор уязвимости: CVE-2023-3935

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

Уязвимый продукт: Siemens Desigo CC: 5.0 - 7.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-625850.txt
- https://bdu.fstec.ru/vul/2023-04985

17

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38076

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05755

18

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38075

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05754

19

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38074

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05753

20

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38073

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05752

21

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38072

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05751

22

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38071

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05750

23

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-38070

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-478780.txt
- https://bdu.fstec.ru/vul/2023-05749

Краткое описание: Выполнение произвольного кода в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2022-37434

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

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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.

24

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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2022-05325

25

Краткое описание: Повышение привилегий в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2022-41032

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

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-06453

26

Краткое описание: Выполнение произвольного кода в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-21808

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-00850

27

Краткое описание: Выполнение произвольного кода в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-24895

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-03210

28

Краткое описание: Выполнение произвольного кода в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-24897

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-03308

29

Краткое описание: Выполнение произвольного кода в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-28260

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-02907

30

Краткое описание: Отказ в обслуживании в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-29331

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-03439

31

Краткое описание: Повышение привилегий в Siemens SINEC PNI

Идентификатор уязвимости: CVE-2023-24936

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

Уязвимый продукт: Siemens SINEC PNI: до 2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-150063.txt
- https://bdu.fstec.ru/vul/2023-03440

32

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC MV500

Идентификатор уязвимости: CVE-2023-35788

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens SIMATIC MV500: до 3.3.5

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-099606.txt
- https://bdu.fstec.ru/vul/2023-03498

33

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC MV500

Идентификатор уязвимости: CVE-2022-23219

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

Уязвимый продукт: Siemens SIMATIC MV500: до 3.3.5

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: 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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-099606.txt
- https://bdu.fstec.ru/vul/2022-01633

34

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC MV500

Идентификатор уязвимости: CVE-2022-23218

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

Уязвимый продукт: Siemens SIMATIC MV500: до 3.3.5

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: 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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-099606.txt
- https://bdu.fstec.ru/vul/2022-01632

Краткое описание: Выполнение произвольного кода в Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-29245

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

Уязвимый продукт: Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices:
Guardian: до 23.1.0
Central Management Console: до 23.1.0
RUGGEDCOM APE1808: All versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

35 **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: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://security.nozominetworks.com/NN-2023:11-01
- http://cert-portal.siemens.com/productcert/txt/ssa-292063.txt

36

Краткое описание: Отказ в обслуживании в Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-32649

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices:
Guardian: до 23.1.0
Central Management Console: до 23.1.0
RUGGEDCOM APE1808: All versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://security.nozominetworks.com/NN-2023:10-01
- http://cert-portal.siemens.com/productcert/txt/ssa-292063.txt

Краткое описание: Выполнение произвольного кода в Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices

Идентификатор уязвимости: CVE-2023-2567

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

Уязвимый продукт: Nozomi Networks Guardian and CMC, Siemens RUGGEDCOM APE1808 devices:
Guardian: до 23.1.0
Central Management Console: до 23.1.0
RUGGEDCOM APE1808: All versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

37 **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: 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://security.nozominetworks.com/NN-2023:9-01
- http://cert-portal.siemens.com/productcert/txt/ssa-292063.txt

38

Краткое описание: Выполнение произвольного кода в Wireshark

Идентификатор уязвимости: None

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

Уязвимый продукт: Wireshark: 3.6.0 - 4.0.10

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-16 / 2023-11-16

Ссылки на источник:

- http://www.wireshark.org/security/wnpa-sec-2023-29.html
- http://gitlab.com/wireshark/wireshark/-/issues/19404

39

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2023-44436

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Kofax Power PDF Advanced: до 5.0.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1608/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.15.htm

40

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2023-44435

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Kofax Power PDF Advanced: до 5.0.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1607/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.15.htm

41

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2023-44432

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Kofax Power PDF Advanced: до 5.0.0.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1606/
- http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.15.htm