НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-15.1 | 15 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-46156	Siemens SIMATIC S7-1500 CPUs	Сетевой	DoS	2023-12-15	✓
2	Высокая	CVE-2023-6705	Microsoft Edge	Сетевой	ACE	2023-12-15	✓
3	Высокая	CVE-2023-6704	Microsoft Edge	Сетевой	ACE	2023-12-15	✓
4	Высокая	CVE-2023-6703	Microsoft Edge	Сетевой	ACE	2023-12-15	✓
5	Высокая	CVE-2023-6702	Microsoft Edge	Сетевой	ACE	2023-12-15	✓
6	Высокая	CVE-2023-6706	Microsoft Edge	Сетевой	ACE	2023-12-15	✓
7	Критическая	CVE-2023-6553	Backup Migration Plugin for WordPress	Сетевой	ACE	2023-12-13	✓
8	Критическая	CVE-2023-6316	MW WP Form plugin for WordPress	Сетевой	WLF	2023-12-14	✓
9	Высокая	CVE-2023-48427	Siemens SINEC INS	Сетевой	PE	2023-12-14	✓
10	Высокая	CVE-2023-0464	Siemens SINEC INS	Сетевой	DoS	2023-12-14	✓
11	Критическая	CVE-2022-36323	Siemens SCALANCE M-800/S615 Family	Сетевой	ACE	2023-12-14	✓
12	Критическая	CVE-2023-44373	Siemens SCALANCE M-800/S615 Family	Сетевой	ACE	2023-12-14	✓
13	Высокая	CVE-2023-28831	Siemens SINUMERIK ONE and SINUMERIK MC	Сетевой	DoS	2023-12-13	✓

14	Высокая	CVE-2023-38380	Siemens Industrial Products	Сетевой	DoS	2023-12-13	✓
15	Высокая	CVE-2022-47375	Siemens Industrial Products	Сетевой	DoS	2023-12-13	✓
16	Высокая	CVE-2022-47374	Siemens Industrial Products	Сетевой	DoS	2023-12-13	✓
17	Высокая	CVE-2023-46156	Siemens SINUMERIK ONE and SINUMERIK MC	Сетевой	DoS	2023-12-13	✗
18	Высокая	CVE-2023-46285	Siemens User Management Component (UMC)	Сетевой	DoS	2023-12-13	✓
19	Высокая	CVE-2023-46284	Siemens User Management Component (UMC)	Сетевой	DoS	2023-12-13	✓
20	Высокая	CVE-2023-46283	Siemens User Management Component (UMC)	Сетевой	DoS	2023-12-13	✓

1

Краткое описание: Отказ в обслуживании в SIPLUS S7-1500 CPU 1518HF-4 PN (6AG1518-4JP00-4AB0)

Идентификатор уязвимости: CVE-2023-46156

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SIPLUS S7-1500 CPU 1518HF-4 PN (6AG1518-4JP00-4AB0): все версии
SIPLUS S7-1500 CPU 1517H-3 PN (6AG1517-3HP00-4AB0): все версии
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0): все версии
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0): все версии
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0): все версии
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0): все версии
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN00-2AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-7AB0): все версии
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-2AB0): все версии
SIPLUS S7-1500 CPU 1515R-2 PN TX RAIL (6AG2515-2RM00-4AB0): все версии
SIPLUS S7-1500 CPU 1515R-2 PN (6AG1515-2RM00-7AB0): все версии
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0): все версии
SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0): все версии
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0): все версии
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0): все версии
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0): все версии
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0): все версии
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL00-2AB0): все версии
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0): все версии
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0): все версии
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0): все версии
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0): все версии
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL00-2AB0): все версии
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0): все версии

SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0): все версии
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK00-2AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0): все версии
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK00-2AB0): все версии
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0): все версии
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0): все версии
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0): все версии
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0): все версии
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0): все версии
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0): все версии
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0): все версии
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0): все версии
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK00-2AB0): все версии
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0): все версии
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0): все версии
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0): все версии
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0): все версии
SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0): все версии
SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0): все версии
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0): все версии
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0): все версии
SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0): все версии
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0): все версии
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0): все версии
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0): все версии
SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0): все версии
SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0): все версии

SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0): все версии
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0): все версии
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN00-0AB0): все версии
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0): все версии
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0): все версии
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN00-0AB0): все версии
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0): все версии
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0): все версии
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RN03-0AB0): все версии
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0): все версии
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0): все версии
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0): все версии
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM00-0AB0): все версии
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0): все версии
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0): все версии
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM00-0AB0): все версии
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RM03-0AB0): все версии
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0): все версии
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0): все версии
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0): все версии
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL00-0AB0): все версии
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0): все версии
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL00-0AB0): все версии
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0): все версии
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK00-0AB0): все версии
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0): все версии
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0): все версии
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK00-0AB0): все версии
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0): все версии
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0): все версии
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0): все версии
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0): все версии
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0): все версии
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0): все версии

SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK00-0AB0): все версии
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0): все версии
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0): все версии
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0): все версии
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0): все версии
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK00-0AB0): все версии
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): все версии
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ00-0AB0): все версии
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): все версии
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ00-0AB0): все версии
SIMATIC ET 200SP Open Controller CPU 1515SP PC2: все версии
SIMATIC S7-1500 Software Controller: все версии
SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0): до 3.1.0
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0): до 3.1.0
SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0): до 3.1.0
SIMATIC S7-PLCSIM Advanced: до 6.0
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0): до 3.1.0
SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0): до 3.1.0
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP01-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FP03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AP03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FN03-0AB0): до 3.1.0

SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1514SP-2 PN (6ES7514-2DN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DM03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CM03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UL03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TL03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CL03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DK03-0AB0): до 3.1.0
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0): до 3.1.0
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): до 3.1.0
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): до 3.1.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-592380.txt

- https://bdu.fstec.ru/vul/2023-08668

2

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-6705

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 120.0.2210.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6705
- https://bdu.fstec.ru/vul/2023-08755

3

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-6704

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 120.0.2210.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6704
- https://bdu.fstec.ru/vul/2023-08754

4

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-6703

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 120.0.2210.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6703
- https://bdu.fstec.ru/vul/2023-08757

5

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-6702

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 120.0.2210.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6702
- https://bdu.fstec.ru/vul/2023-08756

6

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-6706

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 120.0.2210.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2023-12-15 / 2023-12-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6706
- https://bdu.fstec.ru/vul/2023-08751

Краткое описание: Выполнение произвольного кода в Backup Migration Plugin for WordPress

Идентификатор уязвимости: CVE-2023-6553

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Backup Migration Plugin for WordPress: до 1.3.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Внедрение PHP-кода.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-13 / 2023-12-13

Ссылки на источник:

- https://www.wordfence.com/blog/2023/12/critical-unauthenticated-remote-code-execution-found-in-backup-migration-plugin/

Краткое описание: Запись локальных файлов в MW WP Form

Идентификатор уязвимости: CVE-2023-6316

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: MW WP Form: 5.0.0 - 5.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: запись локальных файлов

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

Оценка CVSSv3: 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: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU97876221/index.html

Краткое описание: Повышение привилегий в SINEC INS

Идентификатор уязвимости: CVE-2023-48427

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: SINEC INS: до 1.0 SP2 Update 2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Перехват учетных данных, отправляемых на сервер.

Последствия эксплуатации: повышение привилегий

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

Оценка CVSSv3: 8.1 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: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-077170.txt

10

Краткое описание: Отказ в обслуживании в SINEC INS

Идентификатор уязвимости: CVE-2023-0464

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

Уязвимый продукт: SINEC INS: до 1.0 SP2 Update 2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование специально созданного вредоносного сертификата.

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: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-077170.txt
- https://bdu.fstec.ru/vul/2023-02108

11

Краткое описание: Выполнение произвольного кода в SCALANCE S615 EEC

Идентификатор уязвимости: CVE-2022-36323

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: SCALANCE S615 EEC: до 8.0
SCALANCE M812-1 ADSL-Router (Annex A): до 8.0
SCALANCE S615: до 8.0
SCALANCE MUM856-1 (RoW): до 8.0
SCALANCE MUM856-1 (EU): до 8.0
SCALANCE MUM853-1 (EU): до 8.0
SCALANCE M876-4 (NAM): до 8.0
SCALANCE M876-4 (EU): до 8.0
SCALANCE M876-4: до 8.0
SCALANCE M876-3 (ROK): до 8.0
SCALANCE M876-3 (EVDO): до 8.0
SCALANCE M874-3: до 8.0
SCALANCE M874-2: до 8.0
SCALANCE M826-2 SHDSL-Router: до 8.0
SCALANCE M816-1 ADSL-Router (Annex B): до 8.0
SCALANCE M816-1 ADSL-Router (Annex A): до 8.0
SCALANCE M812-1 ADSL-Router (Annex B): до 8.0
SCALANCE M804PB: до 8.0
RUGGEDCOM RM1224 LTE(4G) NAM: до 8.0
RUGGEDCOM RM1224 LTE(4G) EU: до 8.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-180704.txt
- https://bdu.fstec.ru/vul/2022-04992

12

Краткое описание: Выполнение произвольного кода в SCALANCE S615 EEC

Идентификатор уязвимости: CVE-2023-44373

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: SCALANCE S615 EEC: до 8.0
SCALANCE M812-1 ADSL-Router (Annex A): до 8.0
SCALANCE S615: до 8.0
SCALANCE MUM856-1 (RoW): до 8.0
SCALANCE MUM856-1 (EU): до 8.0
SCALANCE MUM853-1 (EU): до 8.0
SCALANCE M876-4 (NAM): до 8.0
SCALANCE M876-4 (EU): до 8.0
SCALANCE M876-4: до 8.0
SCALANCE M876-3 (ROK): до 8.0
SCALANCE M876-3 (EVDO): до 8.0
SCALANCE M874-3: до 8.0
SCALANCE M874-2: до 8.0
SCALANCE M826-2 SHDSL-Router: до 8.0
SCALANCE M816-1 ADSL-Router (Annex B): до 8.0
SCALANCE M816-1 ADSL-Router (Annex A): до 8.0
SCALANCE M812-1 ADSL-Router (Annex B): до 8.0
SCALANCE M804PB: до 8.0
RUGGEDCOM RM1224 LTE(4G) NAM: до 8.0
RUGGEDCOM RM1224 LTE(4G) EU: до 8.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-180704.txt
- https://bdu.fstec.ru/vul/2023-08014

Краткое описание: Отказ в обслуживании в SINUMERIK ONE

Идентификатор уязвимости: CVE-2023-28831

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

Уязвимый продукт: SINUMERIK ONE: до 6.22
SINUMERIK MC: до 1.22

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-118850.txt
- https://bdu.fstec.ru/vul/2023-05954

14

Краткое описание: Отказ в обслуживании в SIMATIC CP 1242-7 V2

Идентификатор уязвимости: CVE-2023-38380

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

Уязвимый продукт: SIMATIC CP 1242-7 V2: все версии
SIMATIC CP 1243-1: все версии
SIMATIC CP 1243-1 DNP3: все версии
SIMATIC CP 1243-1 IEC: все версии
SIMATIC CP 1243-7 LTE: все версии
SIMATIC CP 1243-8 IRC: все версии
SIMATIC CP 1543-1: все версии
SINAMICS S210: 6.1
SIPLUS NET CP 1543-1: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-693975.pdf

15

Краткое описание: Отказ в обслуживании в SIMATIC S7-400 CPU 412-2 PN V7

Идентификатор уязвимости: CVE-2022-47375

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

Уязвимый продукт: SIMATIC S7-400 CPU 412-2 PN V7: все версии
SIMATIC S7-400 CPU 414-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 414F-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 416-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 416F-3 PN/DP V7: все версии
SIMATIC PC-Station Plus: все версии
SIPLUS S7-400 CPU 414-3 PN/DP V7: все версии
SIPLUS S7-400 CPU 416-3 PN/DP V7: все версии
SINAMICS S120: до 5.2 SP3 HF15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-892915.pdf

16

Краткое описание: Отказ в обслуживании в SIMATIC S7-400 CPU 412-2 PN V7

Идентификатор уязвимости: CVE-2022-47374

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: SIMATIC S7-400 CPU 412-2 PN V7: все версии
SIMATIC S7-400 CPU 414-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 414F-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 416-3 PN/DP V7: все версии
SIMATIC S7-400 CPU 416F-3 PN/DP V7: все версии
SIMATIC PC-Station Plus: все версии
SIPLUS S7-400 CPU 414-3 PN/DP V7: все версии
SIPLUS S7-400 CPU 416-3 PN/DP V7: все версии
SINAMICS S120: до 5.2 SP3 HF15

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-892915.pdf

17

Краткое описание: Отказ в обслуживании в SINUMERIK MC

Идентификатор уязвимости: CVE-2023-46156

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SINUMERIK MC: все версии
SINUMERIK ONE: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-280603.pdf

18

Краткое описание: Отказ в обслуживании в Opcenter Quality

Идентификатор уязвимости: CVE-2023-46285

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Opcenter Quality: все версии
SINUMERIK Integrate RunMyHMI /Automotive: все версии
Totally Integrated Automation Portal (TIA Portal): 14 - 18
SIMATIC PCS neo: до 4.1
User Management Component (UMC): до 2.11.2

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: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-999588.pdf

19

Краткое описание: Отказ в обслуживании в Opcenter Quality

Идентификатор уязвимости: CVE-2023-46284

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

Уязвимый продукт: Opcenter Quality: все версии
SINUMERIK Integrate RunMyHMI /Automotive: все версии
Totally Integrated Automation Portal (TIA Portal): 14 - 18
SIMATIC PCS neo: до 4.1
User Management Component (UMC): до 2.11.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-999588.pdf

20

Краткое описание: Отказ в обслуживании в Opcenter Quality

Идентификатор уязвимости: CVE-2023-46283

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

Уязвимый продукт: Opcenter Quality: все версии
SINUMERIK Integrate RunMyHMI /Automotive: все версии
Totally Integrated Automation Portal (TIA Portal): 14 - 18
SIMATIC PCS neo: до 4.1
User Management Component (UMC): до 2.11.2
External links
http://cert-portal.siemens.com/productcert/pdf/ssa-999588.pdf
Q & A
Can this vulnerability be exploited remotely?
Yes. This vulnerability can be exploited by a remote non-authenticated attacker via the Internet.
How the attacker can exploit this vulnerability?
The attacker would have to send a specially crafted request to the affected application in order to exploit this vulnerability.
Is there known malware, which exploits this vulnerability?
No. We are not aware of malware exploiting this vulnerability.

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-13 / 2023-12-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-999588.pdf