НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-20.1 | 20 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2022-27405	Siemens RUGGEDCOM APE1808 Product Family	Сетевой	DoS	2023-09-19	✓
2	Высокая	CVE-2022-29275	Siemens RUGGEDCOM APE1808 Product Family	Локальный	ACE	2023-09-19	✓
3	Высокая	CVE-2022-30283	Siemens RUGGEDCOM APE1808 Product Family	Локальный	PE	2023-09-19	✓
4	Высокая	CVE-2022-30772	Siemens RUGGEDCOM APE1808 Product Family	Локальный	ACE	2023-09-19	✓
5	Высокая	CVE-2022-35893	Siemens RUGGEDCOM APE1808 Product Family	Локальный	ACE	2023-09-19	✓
6	Высокая	CVE-2022-35895	Siemens RUGGEDCOM APE1808 Product Family	Локальный	ACE	2023-09-19	✓
7	Высокая	CVE-2022-36338	Siemens RUGGEDCOM APE1808 Product Family	Локальный	ACE	2023-09-19	✓
8	Высокая	CVE-2023-31041	Siemens RUGGEDCOM APE1808 Product Family	Сетевой	OSI	2023-09-19	✓
9	Критическая	CVE-2023-41179	Trend Micro Apex One and Worry-Free Business	Сетевой	ACE	2023-09-19	✓
10	Критическая	CVE-2022-33186	Brocade Fabric OS	Сетевой	ACE	2023-09-20	✓
11	Высокая	CVE-2023-4427	Chrome OS	Сетевой	ACE	2023-09-19	✓

12	Средняя	CVE-2023-36847	Juniper Junos OS	Сетевой	OSI	2023-08-18	✓
13	Средняя	CVE-2023-36846	Juniper Junos OS	Сетевой	OSI	2023-08-18	✓
14	Средняя	CVE-2023-36845	Juniper Junos OS	Сетевой	CI	2023-08-18	✓
15	Средняя	CVE-2023-36844	Juniper Junos OS	Сетевой	ACE	2023-08-18	✓
16	Критическая	CVE-2023-36187	NETGEAR R6400v2	Сетевой	ACE	2023-09-01	✓
17	Высокая	CVE-2023-37284	TP-Link Archer C20	Смежная сеть	ACE	2023-09-06	✓
18	Высокая	CVE-2023-38568	TP-Link Archer A10	Смежная сеть	ACE	2023-09-06	✓
19	Высокая	CVE-2023-4711	D-Link DAR-8000-10	Сетевой	CI	2023-09-01	✓
20	Высокая	CVE-2023-40193	Deco M4	Смежная сеть	ACE	2023-09-06	✓
21	Высокая	CVE-2023-40357	TP-LINK products	Смежная сеть	ACE	2023-09-06	✓
22	Высокая	CVE-2023-30800	MikroTik RouterOS	Сетевой	DoS	2023-09-07	✓
23	Критическая	CVE-2023-36735	Microsoft Edge	Сетевой	ACE	2023-09-18	✓
24	Критическая	CVE-2023-30909	HPE OneView	Сетевой	SB	2023-09-15	✓
25	Критическая	CVE-2023-30908	HPE OneView	Сетевой	SB	2023-09-15	✓

1

Краткое описание: Отказ в обслуживании в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-27405

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

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: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt
- https://bdu.fstec.ru/vul/2022-06917

2

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-29275

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

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

3

Краткое описание: Повышение привилегий в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-30283

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

4

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-30772

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

5

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-35893

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

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

6

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-35895

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

7

Краткое описание: Выполнение произвольного кода в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2022-36338

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

8

Краткое описание: Получение конфиденциальной информации в Siemens RUGGEDCOM APE1808 Product Family

Идентификатор уязвимости: CVE-2023-31041

Идентификатор программной ошибки: CWE-312 Хранение важных данных в незашифрованном виде

Уязвимый продукт: Siemens RUGGEDCOM APE1808 Product Family:
RUGGEDCOM APE1808W10 CC: до 1.0.212N
RUGGEDCOM APE1808W10: до 1.0.212N
RUGGEDCOM APE1808LNX CC: до 1.0.212N
RUGGEDCOM APE1808LNX: до 1.0.212N
RUGGEDCOM APE1808CLA-S5 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S5: до 1.0.212N
RUGGEDCOM APE1808CLA-S3 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S3: до 1.0.212N
RUGGEDCOM APE1808CLA-S1 CC: до 1.0.212N
RUGGEDCOM APE1808CLA-S1: до 1.0.212N
RUGGEDCOM APE1808CLA-P CC: до 1.0.212N
RUGGEDCOM APE1808CLA-P: до 1.0.212N
RUGGEDCOM APE1808 SAM-L CC: до 1.0.212N
RUGGEDCOM APE1808 SAM-L: до 1.0.212N
RUGGEDCOM APE1808 ELAN CC: до 1.0.212N
RUGGEDCOM APE1808 ELAN: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT CC: до 1.0.212N
RUGGEDCOM APE1808 CLOUDCONNECT: до 1.0.212N
RUGGEDCOM APE1808 CKP CC: до 1.0.212N
RUGGEDCOM APE1808 CKP: до 1.0.212N
RUGGEDCOM APE1808 ADM CC: до 1.0.212N
RUGGEDCOM APE1808 ADM: до 1.0.212N

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 7.5 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: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-957369.txt

Краткое описание: Выполнение произвольного кода в Trend Micro Apex One and Worry-Free Business

Идентификатор уязвимости: CVE-2023-41179

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

Уязвимый продукт: Trend Micro Apex One and Worry-Free Business:
Apex One: 2019 - SP1 b11564
Worry-Free Business Security: 9.5 - xg

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

9

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

Оценка CVSSv3: 9.1 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: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://success.trendmicro.com/dcx/s/solution/000294994?language=en_US
- http://files.trendmicro.com/documentation/readme/Apex%20One/2020/apex_one_2019_win_p_b12380_EN_patch_Readme.html
- http://files.trendmicro.com/documentation/wfbs/10.0/WFBS_100_SP1_WIN_ALL_Patch_2495.txt

Краткое описание: Выполнение произвольного кода в Brocade Fabric OS

Идентификатор уязвимости: CVE-2022-33186

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

Уязвимый продукт: Brocade Fabric OS: до 9.1.1a

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-09-20 / 2023-09-20

Ссылки на источник:

- http://www.ibm.com/support/pages/node/6852173

11

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4427

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

Уязвимый продукт: Chrome OS: до 108.0.5359.243

Категория уязвимого продукта: Unix-подобные операционные системы 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: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-19 / 2023-09-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/long-term-support-channel-update-for_18.html
- https://bdu.fstec.ru/vul/2023-04907

12

Краткое описание: Получение конфиденциальной информации в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36847

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

Уязвимый продукт: Juniper Junos OS: до 23.2R1

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

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-18 / 2023-08-18

Ссылки на источник:

- http://supportportal.juniper.net/JSA72300
- https://bdu.fstec.ru/vul/2023-05099

13

Краткое описание: Получение конфиденциальной информации в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36846

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

Уязвимый продукт: Juniper Junos OS: до 23.2R1

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

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-18 / 2023-08-18

Ссылки на источник:

- http://supportportal.juniper.net/JSA72300
- https://bdu.fstec.ru/vul/2023-04852

14

Краткое описание: Внедрение кода в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36845

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Junos OS: до 23.2R1

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

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-18 / 2023-08-18

Ссылки на источник:

- http://supportportal.juniper.net/JSA72300
- https://bdu.fstec.ru/vul/2023-04994

15

Краткое описание: Выполнение произвольного кода в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-36844

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Junos OS: до 23.2R1

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-18 / 2023-08-18

Ссылки на источник:

- http://supportportal.juniper.net/JSA72300
- https://bdu.fstec.ru/vul/2023-04993

Краткое описание: Выполнение произвольного кода в NETGEAR R6400v2

Идентификатор уязвимости: CVE-2023-36187

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: NETGEAR R6400v2: до 1.0.4.118

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

16 **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: 2023-09-01 / 2023-09-07

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-36187
- https://bdu.fstec.ru/vul/2023-05160

17

Краткое описание: Выполнение произвольного кода в TP-Link Archer C20

Идентификатор уязвимости: CVE-2023-37284

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: TP-Link Archer C20: до Archer C20(JP)_V1_230616

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-11

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-37284

Краткое описание: Выполнение произвольного кода в TP-Link Archer A10

Идентификатор уязвимости: CVE-2023-38568

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

Уязвимый продукт: TP-Link Archer A10: до Archer A10(JP)_V2_230504

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

18

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-11

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38568

Краткое описание: Внедрение кода в D-Link DAR-8000-10

Идентификатор уязвимости: CVE-2023-4711

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

Уязвимый продукт: D-Link DAR-8000-10: до 20230819.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Внедрение кода

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

Оценка CVSSv3: 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: 2023-09-01 / 2023-09-07

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-4711
- https://bdu.fstec.ru/vul/2023-05203

Краткое описание: Выполнение произвольного кода в Deco M4

Идентификатор уязвимости: CVE-2023-40193

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

Уязвимый продукт: Deco M4: до Deco M4(JP)_V2_1.5.8 Build 20230619

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

20

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-11

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-40193

21

Краткое описание: Выполнение произвольного кода в TP-LINK products

Идентификатор уязвимости: CVE-2023-40357

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

Уязвимый продукт: TP-LINK products:
TP-LINK Archer AX50: до Archer AX50(JP)_V1_230529
TP-LINK Archer A10: до Archer A10(JP)_V2_230504
TP-LINK Archer AX10: до Archer AX10(JP)_V1.2_230508
TP-LINK Archer AX11000: до Archer AX11000(JP)_V1_230523

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-06 / 2023-09-11

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-40357

22

Краткое описание: Отказ в обслуживании в MikroTik RouterOS

Идентификатор уязвимости: CVE-2023-30800

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: MikroTik RouterOS: до 6.49.10 stable

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2023-09-07 / 2023-09-07

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-30800
- https://bdu.fstec.ru/vul/2023-05527

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-36735

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 116.0.1938.81

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 9.6 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: 2023-09-18 / 2023-09-18

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36735

Краткое описание: Обход безопасности в HPE OneView

Идентификатор уязвимости: CVE-2023-30909

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: HPE OneView: до 8.30.01

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

24 **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: 2023-09-15 / 2023-09-15

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04538en_us

Краткое описание: Обход безопасности в HPE OneView

Идентификатор уязвимости: CVE-2023-30908

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: HPE OneView: до 8.30.01

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

25 **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: 2023-09-15 / 2023-09-15

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04530en_us