НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-06.1 | 6 октября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2021-45960	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	DoS	2023-10-06	✓
2	Высокая	CVE-2021-46143	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
3	Критическая	CVE-2022-22822	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
4	Критическая	CVE-2022-22823	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
5	Критическая	CVE-2022-22824	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
6	Высокая	CVE-2022-22825	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
7	Высокая	CVE-2022-22826	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
8	Высокая	CVE-2022-25314	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	DoS	2023-10-06	✓
9	Критическая	CVE-2022-25315	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
10	Критическая	CVE-2022-25235	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓

11	Критическая	CVE-2022-25236	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	DoS	2023-10-06	✓
12	Критическая	CVE-2022-23852	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
13	Высокая	CVE-2022-23990	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
14	Высокая	CVE-2022-22827	Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products	Сетевой	ACE	2023-10-06	✓
15	Высокая	CVE-2023-5344	Vim	Сетевой	ACE	2023-10-04	✓
16	Высокая	CVE-2023-4751	Vim	Локальный	ACE	2023-10-04	✓
17	Высокая	CVE-2023-4734	Vim	Локальный	ACE	2023-10-04	✓
18	Критическая	CVE-2023-20101	Cisco Emergency Responder	Сетевой	PE	2023-10-04	✓
19	Высокая	CVE-2023-20259	Cisco Unified Communications Products	Сетевой	DoS	2023-10-06	✓
20	Высокая	CVE-2023-44466	Linux kernel Ceph filesystem	Сетевой	ACE	2023-10-05	✓
21	Критическая	CVE-2023-38427	Linux kernel ksmbd	Сетевой	ACE	2023-10-05	✓
22	Критическая	CVE-2023-38431	Linux kernel ksmbd	Сетевой	OSI	2023-10-05	✓
23	Высокая	CVE-2023-44410	D-Link D-View	Сетевой	PE	2023-10-05	✗
24	Критическая	CVE-2023-44411	D-Link D-View	Сетевой	OSI	2023-10-05	✗

25	Высокая	CVE-2023-44412	D-Link D-View	Сетевой	RLF	2023-10-05	✗
26	Критическая	CVE-2023-44414	D-Link D-View	Сетевой	ACE	2023-10-05	✗
27	Критическая	CVE-2023-22515	Confluence Server and Data Center	Сетевой	ACE	2023-10-05	✓
28	Высокая	CVE-2023-5346	Microsoft Edge	Сетевой	ACE	2023-10-05	✓
29	Высокая	CVE-2023-4911	Ubuntu, Debian Linux, Fedora	Локальный	ACE	2023-10-03	✓
30	Высокая	CVE-2023-42111	PDF-XChange Editor	Локальный	OSI	2023-10-03	✓
31	Высокая	CVE-2023-42108	PDF-XChange Editor	Локальный	ACE	2023-10-03	✓

Краткое описание: Отказ в обслуживании в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2021-45960

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

1 **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: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01003

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2021-46143

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

2 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.1 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01052

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22822

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

3 **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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-02823

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22823

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

4 **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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01060

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22824

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

5 **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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-00800

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22825

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

6 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-00805

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22826

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

7 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01059

Краткое описание: Отказ в обслуживании в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-25314

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

8 **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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01062

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-25315

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

9 **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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01071

10

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-25235

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01063

Краткое описание: Отказ в обслуживании в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-25236

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

1
1

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01065

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-23852

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

1
2

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01702

13

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-23990

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-00999

14

Краткое описание: Выполнение произвольного кода в Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products

Идентификатор уязвимости: CVE-2022-22827

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

Уязвимый продукт: Hitachi Energy AFS65x, AFF66x, AFS67x and AFR67x Series Products:
AFF66X FW: 03.0.02
AFS670-V20: все версии
AFS66X-B: все версии
AFS660-C: все версии
AFS66X-S: все версии
AFR677: до 09.1.08 FW
AFS67X: до 09.1.08 FW
AFS65X: до 09.1.08 FW

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
- http://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true
- https://bdu.fstec.ru/vul/2022-01058

15

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2023-5344

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

Уязвимый продукт: Vim: до 9.0.1969

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: 7.5 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: 2023-10-04 / 2023-10-04

Ссылки на источник:

- http://huntr.dev/bounties/530cb762-899e-48d7-b50e-dad09eb775bf
- http://github.com/vim/vim/commit/3bd7fa12e146c6051490d048a4acbfba974eeb04

16

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2023-4751

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

Уязвимый продукт: Vim: до 9.0.1331

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: 2023-10-04 / 2023-10-04

Ссылки на источник:

- http://huntr.dev/bounties/db7be8d6-6cb7-4ae5-9c4e-805423afa378
- http://github.com/vim/vim/commit/e1121b139480f53d1b06f84f3e4574048108fa0b
- https://bdu.fstec.ru/vul/2023-05153

17

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2023-4734

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

Уязвимый продукт: Vim: до 9.0.1846

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: 2023-10-04 / 2023-10-04

Ссылки на источник:

- http://github.com/vim/vim/commit/4c6fe2e2ea62469642ed1d80b16d39e616b25cf5
- http://huntr.dev/bounties/688e4382-d2b6-439a-a54e-484780f82217
- https://bdu.fstec.ru/vul/2023-05671

18

Краткое описание: Повышение привилегий в Cisco Emergency Responder

Идентификатор уязвимости: CVE-2023-20101

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Cisco Emergency Responder: 12.5.1SU4

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: 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: 2023-10-04 / 2023-10-04

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cer-priv-esc-B9t3hqk9
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh34565

19

Краткое описание: Отказ в обслуживании в Cisco Unified Communications Products

Идентификатор уязвимости: CVE-2023-20259

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco Unified Communications Products:
Cisco Emergency Responder: 14.0(1.14900.8) - 14SU3
Cisco Prime Collaboration Deployment: 14.0(1.13900.96) - 14SU3
Cisco Unified Communications Manager: 12.5(1)SU7 - 14SU3
Cisco Unified Communications Manager IM & Presence Service: 12.5(1)SU7 - 14SU3
Cisco Unified Communications Manager Session Management Edition: 12.5(1)SU7 - 14SU3
Cisco Unity Connection: 12.5 - 14SU3

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-06 / 2023-10-06

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-apidos-PGsDcdNF

20

Краткое описание: Выполнение произвольного кода в Linux kernel Ceph filesystem

Идентификатор уязвимости: CVE-2023-44466

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

Уязвимый продукт: Linux kernel Ceph filesystem: до 6.4.5

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://github.com/torvalds/linux/commit/a282a2f10539dce2aa619e71e1817570d557fc97
- http://github.com/google/security-research/security/advisories/GHSA-jg27-jx6w-xwph
- http://www.spinics.net/lists/ceph-devel/msg57909.html
- http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a282a2f10539dce2aa619e71e1817570d557fc97

Краткое описание: Выполнение произвольного кода в Linux kernel ksmbd

Идентификатор уязвимости: CVE-2023-38427

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

Уязвимый продукт: Linux kernel ksmbd: до 6.3.8

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.

21

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: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/smb/server?id=f1a411873c85b642f13b01f21b534c2bab81fc1b
- http://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.8
- http://security.netapp.com/advisory/ntap-20230824-0011/
- https://bdu.fstec.ru/vul/2023-03956

Краткое описание: Получение конфиденциальной информации в Linux kernel ksmbd

Идентификатор уязвимости: CVE-2023-38431

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux kernel ksmbd: до 6.3.8

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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

2
2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/smb/server?id=368ba06881c395f1c9a7ba22203cf8d78b4addc0
- http://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.8
- http://security.netapp.com/advisory/ntap-20230824-0011/
- https://bdu.fstec.ru/vul/2023-03952

2
3

Краткое описание: Повышение привилегий в D-Link D-View

Идентификатор уязвимости: CVE-2023-44410

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: D-Link D-View: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1508/

24

Краткое описание: Получение конфиденциальной информации в D-Link D-View

Идентификатор уязвимости: CVE-2023-44411

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: D-Link D-View: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1509/

25

Краткое описание: Чтение локальных файлов в D-Link D-View

Идентификатор уязвимости: CVE-2023-44412

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: D-Link D-View: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: чтение локальных файлов

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1510/

26

Краткое описание: Выполнение произвольного кода в D-Link D-View

Идентификатор уязвимости: CVE-2023-44414

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

Уязвимый продукт: D-Link D-View: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1512/

27

Краткое описание: Выполнение произвольного кода в Confluence Server and Data Center

Идентификатор уязвимости: CVE-2023-22515

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Confluence Server and Data Center: 8.0.0 - 8.5.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://jira.atlassian.com/browse/CONFSERVER-92457
- http://confluence.atlassian.com/display/KB/FAQ+for+CVE-2023-22515
- http://confluence.atlassian.com/pages/viewpage.action?pageId=1295682276
- http://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

28

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-5346

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 117.0.2045.47

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-05 / 2023-10-05

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-5346

29

Краткое описание: Выполнение произвольного кода в Ubuntu, Debian Linux, Fedora

Идентификатор уязвимости: CVE-2023-4911

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

Уязвимый продукт: Ubuntu, Debian Linux, Fedora:
Ubuntu: 22.04 - 23.04
libc6 (Ubuntu package): before 2.37-0ubuntu2.1

Debian Linux: All versions
glibc (Debian package): before 2.36-9+deb12u3

Fedora: 39
glibc: before 2.38-6.fc39

Fedora: 37
glibc: before 2.36-14.fc37

Fedora: 38
glibc: before 2.37-10.fc38

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

Способ эксплуатации: Отправка специально сформированного запроса.

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: 2023-10-03 / 2023-10-03

Ссылки на источник:

- http://www.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-escalation-glibc-ld-so.txt
- http://ubuntu.com/security/notices/USN-6409-1
- http://www.debian.org/security/2023/dsa-5514
- http://bodhi.fedoraproject.org/updates/FEDORA-2023-63e5a77522
- http://bodhi.fedoraproject.org/updates/FEDORA-2023-028062484e
- http://bodhi.fedoraproject.org/updates/FEDORA-2023-2b8c11ee75

30

Краткое описание: Получение конфиденциальной информации в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-42111

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PDF-XChange Editor: 10.1.0.380
PDF-Tools: 10.1.0.380
PDF-XChange PRO: 10.1.0.380

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем 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: 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: 2023-10-03 / 2023-10-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1481/
- http://www.tracker-software.com/support/security-bulletins.html

31

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-42108

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PDF-XChange Editor: 10.1.0.380
PDF-Tools: 10.1.0.380
PDF-XChange PRO: 10.1.0.380

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: 2023-10-03 / 2023-10-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1483/
- http://www.tracker-software.com/support/security-bulletins.html