НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-12.1 | 12 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-20271	Cisco Evolved Programmable Network Manager and Cisco Prime Infrastructure	Сетевой	ACE	2024-01-11	✓
2	Критическая	CVE-2023-5356	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	OSI	2024-01-12	✓
3	Критическая	CVE-2023-7028	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	OSI	2024-01-12	✓
4	Критическая	CVE-2024-20272	Cisco Unity Connection	Сетевой	WLF	2024-01-11	✓
5	Критическая	CVE-2023-51102	Tenda W9	Сетевой	DoS	2023-12-26	✗
6	Критическая	CVE-2023-51101	Tenda W9	Сетевой	DoS	2023-12-26	✗
7	Критическая	CVE-2023-51099	Tenda W9	Сетевой	DoS	2023-12-26	✗
8	Критическая	CVE-2023-51098	Tenda W9	Сетевой	DoS	2023-12-26	✗
9	Критическая	CVE-2023-51097	Tenda W9	Сетевой	DoS	2023-12-26	✗
10	Критическая	CVE-2023-51091	Tenda M3	Сетевой	DoS	2023-12-26	✗
11	Критическая	CVE-2023-50990	Tenda M3	Сетевой	DoS	2023-12-26	✗
12	Критическая	CVE-2023-7095	TOTOLINK A7100RU	Сетевой	ACE	2023-12-18	✗
13	Критическая	CVE-2023-51093	Tenda M3	Сетевой	DoS	2023-12-26	✗

14	Критическая	CVE-2023-51095	Tenda M3	Сетевой	DoS	2023-12-26	✕
15	Критическая	CVE-2023-50983	Tenda i29	Сетевой	DoS	2023-12-20	✕
16	Критическая	CVE-2023-50992	Tenda i29	Сетевой	DoS	2023-12-20	✕
17	Критическая	CVE-2023-50989	Tenda i29	Сетевой	DoS	2023-12-20	✕
18	Критическая	CVE-2023-50988	Tenda i29	Сетевой	DoS	2023-12-20	✕
19	Критическая	CVE-2023-50987	Tenda i29	Сетевой	DoS	2023-12-20	✕
20	Критическая	CVE-2023-50986	Tenda i29	Сетевой	DoS	2023-12-20	✕
21	Критическая	CVE-2023-50985	Tenda i29	Сетевой	DoS	2023-12-20	✕
22	Критическая	CVE-2023-50984	Tenda i29	Сетевой	DoS	2023-12-20	✕
23	Критическая	CVE-2023-49004	D-Link DIR-850L	Сетевой	ACE	2023-12-19	✕

1

Краткое описание: Выполнение произвольного кода в Cisco Evolved Programmable Network Manager and Cisco Prime Infrastructure

Идентификатор уязвимости: CVE-2023-20271

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

Уязвимый продукт: Evolved Programmable Network (EPN) Manager: 7.0 - 7.1
Cisco Prime Infrastructure: 3.9 - 3.10

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-11 / 2024-01-11

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq

2

Краткое описание: Получение конфиденциальной информации в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2023-5356

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Gitlab Community Edition: 8.13 - 16.7.1
GitLab Enterprise Edition: 8.13.0 - 16.7.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/

3

Краткое описание: Получение конфиденциальной информации в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2023-7028

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Gitlab Community Edition: 16.1.0 - 16.7.1
GitLab Enterprise Edition: 16.1.0 - 16.7.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-12 / 2024-01-12

Ссылки на источник:

- http://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/

4

Краткое описание: Запись локальных файлов в Cisco Unity Connection

Идентификатор уязвимости: CVE-2024-20272

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

Уязвимый продукт: Cisco Unity Connection: 12.5 - 14.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: запись локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-11 / 2024-01-11

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

5

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2023-51102

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-00100

6

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2023-51101

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

7

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2023-51099

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

Уязвимый продукт: Tenda W9: версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

8

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2023-51098

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

Уязвимый продукт: Tenda W9: версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

9

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2023-51097

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda W9: версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda M3

Идентификатор уязвимости: CVE-2023-51091

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda M3: до версии 1.0.0.12(4856).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

10 **Последствия эксплуатации:** отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

11

Краткое описание: Отказ в обслуживании в Tenda M3

Идентификатор уязвимости: CVE-2023-50990

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda M3: до версии 1.0.0.12(4856).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

12

Краткое описание: Выполнение произвольного кода в TOTOLINK A7100RU

Идентификатор уязвимости: CVE-2023-7095

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

Уязвимый продукт: TOTOLINK A7100RU: версии 7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-18 / 2023-12-18

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-00060

13

Краткое описание: Отказ в обслуживании в Tenda M3

Идентификатор уязвимости: CVE-2023-51093

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda M3: до версии 1.0.0.12(4856).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda M3

Идентификатор уязвимости: CVE-2023-51095

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda M3: до версии 1.0.0.12(4856).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

14 **Последствия эксплуатации:** отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-26 / 2023-12-29

Ссылки на источник:

15

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50983

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

16

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50992

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

17

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50989

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50988

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

18 **Последствия эксплуатации:** отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

19

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50987

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

20

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50986

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

21

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50985

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

22

Краткое описание: Отказ в обслуживании в Tenda i29

Идентификатор уязвимости: CVE-2023-50984

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i29: до версии 1.0.0.5.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-20 / 2023-12-22

Ссылки на источник:

23

Краткое описание: Выполнение произвольного кода в D-Link DIR-850L

Идентификатор уязвимости: CVE-2023-49004

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

Уязвимый продукт: D-Link DIR-850L: версии B1_FW223WWb01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-12-19 / 2023-12-22

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-08998