НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-03-04.1 | 4 марта 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-0387	MOXA EDS-4000/G4000	Смежная сеть	LoI	2024-02-26	✓
2	Высокая	CVE-2023-42788	Fortinet FortiManager and FortiAnalyzer	Локальный	ACE	2023-10-12	✓
3	Высокая	CVE-2023-42791	Fortinet FortiManager and FortiAnalyzer	Сетевой	RLF	2023-10-12	✓
4	Высокая	CVE-2023-29181	Fortinet FortiOS	Сетевой	ACE	2023-06-13	✓
5	Высокая	CVE-2023-29180	Fortinet FortiOS	Сетевой	DoS	2023-06-13	✓
6	Критическая	CVE-2024-27905	Apache Aurora	Сетевой	OSI	2024-03-01	✗
7	Критическая	CVE-2024-25128	Apache Airflow	Сетевой	SB	2024-03-01	✓
8	Высокая	CVE-2024-1939	Microsoft Edge	Сетевой	ACE	2024-02-29	✓
9	Высокая	CVE-2024-25578	MicroDicom DICOM Viewer	Локальный	ACE	2024-03-01	✓
10	Высокая	CVE-2024-22100	MicroDicom DICOM Viewer	Локальный	ACE	2024-03-01	✓
11	Высокая	CVE-2024-1938	Microsoft Edge	Сетевой	ACE	2024-02-29	✓
12	Высокая	CVE-2024-1941	Delta Electronics CNCSoft-B	Локальный	ACE	2024-03-01	✓
13	Высокая	CVE-2024-20321	Cisco NX-OS Software	Сетевой	DoS	2024-02-29	✓

14	Высокая	CVE-2024-20267	Cisco NX-OS Software	Сетевой	DoS	2024-02-29	✓
15	Высокая	CVE-2023-25221	libde265	Локальный	ACE	2024-02-28	✓
16	Критическая	CVE-2024-22857	zlog	Сетевой	ACE	2024-02-28	✗
17	Высокая	CVE-2024-1453	Santesoft Sante DICOM Viewer Pro	Сетевой	OSI	2024-02-28	✓
18	Критическая	CVE-2023-24331	D-Link Dir 816	Сетевой	ACE	2024-02-27	✗
19	Высокая	CVE-2024-21836	llama.cpp	Сетевой	ACE	2024-02-27	✓
20	Высокая	CVE-2024-21802	llama.cpp	Сетевой	ACE	2024-02-27	✓
21	Высокая	CVE-2024-21825	llama.cpp	Сетевой	ACE	2024-02-27	✓
22	Высокая	CVE-2024-23496	llama.cpp	Сетевой	ACE	2024-02-27	✓
23	Высокая	CVE-2024-23605	llama.cpp	Сетевой	ACE	2024-02-27	✓
24	Критическая	CVE-2024-1863	Sante PACS Server	Сетевой	ACE	2024-02-26	✓

1

Краткое описание: Потеря целостности в MOXA EDS-4000/G4000

Идентификатор уязвимости: CVE-2024-0387

Идентификатор программной ошибки: CWE-441 Непредусмотренный прокси или посредник ("подмена заместителя")

Уязвимый продукт: MOXA EDS-4000/G4000: до версии 3.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: потеря целостности

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-26 / 2024-02-26

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-01597

2

Краткое описание: Выполнение произвольного кода в Fortinet FortiManager and FortiAnalyzer

Идентификатор уязвимости: CVE-2023-42788

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

Уязвимый продукт: FortiAnalyzer и FortiManager:
FortiAnalyzer: 6.2.0 - 7.4.0
FortiManager: 6.2.0 - 7.4.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-12 / 2023-10-12

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-167
- https://bdu.fstec.ru/vul/2023-06698

3

Краткое описание: Чтение локальных файлов в Fortinet FortiManager and FortiAnalyzer

Идентификатор уязвимости: CVE-2023-42791

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

Уязвимый продукт: FortiManager и FortiAnalyzer:
FortiManager: до версии 7.4.0
FortiAnalyzer: до версии 7.4.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: чтение локальных файлов

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

Оценка CVSSv3: 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: 2023-10-12 / 2023-10-12

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-23-189

4

Краткое описание: Выполнение произвольного кода в Fortinet FortiOS

Идентификатор уязвимости: CVE-2023-29181

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: FortiOS: с версии 4.1.1 по 7.2.4

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-23-119
- https://bdu.fstec.ru/vul/2023-03509

Краткое описание: Отказ в обслуживании в Fortinet FortiOS

Идентификатор уязвимости: CVE-2023-29180

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: FortiOS и FortiProxy:
FortiOS: до версии 7.2.4
FortiProxy: до версии 7.2.3

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: отказ в обслуживании

5

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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-23-111
- https://bdu.fstec.ru/vul/2023-03351

6

Краткое описание: Получение конфиденциальной информации в Apache Aurora

Идентификатор уязвимости: CVE-2024-27905

Идентификатор программной ошибки: CWE-310 Уязвимости, связанные с криптографией

Уязвимый продукт: Apache Aurora: с версии 0.5.0 по 0.22.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-01 / 2024-03-01

Ссылки на источник:

- http://lists.apache.org/thread/564kbv3wqdzkscmdn2bg4vlk48qymryp
- http://www.openwall.com/lists/oss-security/2024/02/27/3

7

Краткое описание: Обход безопасности в Apache Airflow

Идентификатор уязвимости: CVE-2024-25128

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Apache Airflow: с версии 2.0.0 по 2.8.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: обход безопасности

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:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-01 / 2024-03-01

Ссылки на источник:

- http://github.com/dpgaspar/Flask-AppBuilder/security/advisories/GHSA-j2pw-vp55-fqqj
- http://github.com/dpgaspar/Flask-AppBuilder/commit/6336456d83f8f111c842b2b53d1e89627f2502c8

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1939

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

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 122.0.2365.59

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: 2024-02-29 / 2024-02-29

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1939

Краткое описание: Выполнение произвольного кода в MicroDicom DICOM Viewer

Идентификатор уязвимости: CVE-2024-25578

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: MicroDicom DICOM Viewer: с версии 0.0.1 по 2023.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-03-01 / 2024-03-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-060-01

Краткое описание: Выполнение произвольного кода в MicroDicom DICOM Viewer

Идентификатор уязвимости: CVE-2024-22100

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

Уязвимый продукт: MicroDicom DICOM Viewer: с версии 0.0.1 по 2023.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-03-01 / 2024-03-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-060-01

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1938

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

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 122.0.2365.59

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: выполнение произвольного кода

11 **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: 2024-02-29 / 2024-02-29

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1938

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-B

Идентификатор уязвимости: CVE-2024-1941

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-B: 1.0.0.0 - 1.0.0.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

12 **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: 2024-03-01 / 2024-03-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-060-01

Краткое описание: Отказ в обслуживании в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2024-20321

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

Уязвимый продукт: Cisco NX-OS: с версии 7.0(3)F1(1) по 10.4(1)
Cisco Nexus 3600 Platform Switches: все версии
Cisco Nexus 9500 R-Series: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправки специально сформированного eBGP-трафика

Последствия эксплуатации: отказ в обслуживании

13

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

Оценка CVSSv3: 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: 2024-02-29 / 2024-02-29

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ
- https://bdu.fstec.ru/vul/2024-01671

Краткое описание: Отказ в обслуживании в Cisco NX-OS Software

Идентификатор уязвимости: CVE-2024-20267

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

Уязвимый продукт: Cisco NX-OS: с версии 6.0(2)A3(1) по 10.4(1)
Cisco Nexus 3000 Series Switches: все версии
Nexus 5500 Platform Switches: все версии
Nexus 5600 Platform Switches: все версии
Nexus 6000 Series Switches: все версии
Nexus 7000 Series Switches: все версии
Cisco Nexus 9000 Series Switches NX-OS Mode: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

14 **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: 2024-02-29 / 2024-02-29

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM

15

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-25221

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

Уязвимый продукт: libde265: с версии 0.1 по 1.0.10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-28 / 2024-02-28

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/388
- http://lists.debian.org/debian-lts-announce/2023/03/msg00004.html
- https://bdu.fstec.ru/vul/2023-04826

Краткое описание: Выполнение произвольного кода в zlog

Идентификатор уязвимости: CVE-2024-22857

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

Уязвимый продукт: zlog: с версии 0.9.1 по 1.2.17

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

16

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/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-28 / 2024-02-28

Ссылки на источник:

- http://github.com/HardySimpson/zlog/issues/250

17

Краткое описание: Получение конфиденциальной информации в Santesoft Sante DICOM Viewer Pro

Идентификатор уязвимости: CVE-2024-1453

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: DICOM Viewer Pro: 14.0.3

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-28 / 2024-02-28

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-058-01

18

Краткое описание: Выполнение произвольного кода в D-Link Dir 816

Идентификатор уязвимости: CVE-2023-24331

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

Уязвимый продукт: DIR-816: 1.10CNB04

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://github.com/caoyebo/CVE/tree/main/Dlink%20816%20-%20CVE-2023-24331

Краткое описание: Выполнение произвольного кода в llama.cpp

Идентификатор уязвимости: CVE-2024-21836

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

Уязвимый продукт: llama.cpp: 18c2e17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного 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: 8.8 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: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1915

Краткое описание: Выполнение произвольного кода в llama.cpp

Идентификатор уязвимости: CVE-2024-21802

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

Уязвимый продукт: llama.cpp: 18c2e17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.8 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: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1914

Краткое описание: Выполнение произвольного кода в llama.cpp

Идентификатор уязвимости: CVE-2024-21825

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

Уязвимый продукт: llama.cpp: 18c2e17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

21 **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: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1912

Краткое описание: Выполнение произвольного кода в llama.cpp

Идентификатор уязвимости: CVE-2024-23496

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

Уязвимый продукт: llama.cpp: 18c2e17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

22 **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: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1913

Краткое описание: Выполнение произвольного кода в llama.cpp

Идентификатор уязвимости: CVE-2024-23605

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

Уязвимый продукт: llama.cpp: 18c2e17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-27 / 2024-02-27

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2024-1916

Краткое описание: Выполнение произвольного кода в Sante PACS Server

Идентификатор уязвимости: CVE-2024-1863

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

Уязвимый продукт: PACS Server: до 3.3.6

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-26 / 2024-02-26

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-193/