НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-02-26.1 | 26 февраля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-21554	Mitsubishi Electric Electrical Discharge Machines	Сетевой	ACE	2024-02-26	✗
2	Высокая	CVE-2024-1672	Microsoft Edge	Сетевой	OSI	2024-02-26	✓
3	Высокая	CVE-2024-26192	Microsoft Edge	Сетевой	OSI	2024-02-26	✓
4	Высокая	CVE-2024-1595	Delta Electronics CNCSoft-B and DOPSoft	Сетевой	ACE	2024-02-23	✓
5	Критическая	CVE-2024-21767	Commend WS203VICM	Сетевой	OSI	2024-02-23	✓
6	Высокая	CVE-2024-22182	Commend WS203VICM	Сетевой	DoS	2024-02-23	✓
7	Критическая	CVE-2023-52356	LibTIFF	Сетевой	ACE	2024-02-23	✓
8	Критическая	CVE-2023-52355	LibTIFF	Сетевой	ACE	2024-02-23	✓
9	Критическая	CVE-2023-6228	LibTIFF	Сетевой	ACE	2024-02-23	✓
10	Высокая	CVE-2024-6817	Google ChromeOS TLS	Локальный	PE	2024-02-22	✓
11	Высокая	CVE-2024-0611	Google ChromeOS TLS	Локальный	PE	2024-02-22	✓
12	Высокая	CVE-2024-0646	Google ChromeOS TLS	Локальный	PE	2024-02-22	✓
13	Высокая	CVE-2024-20672	Tenable Identity Exposure	Сетевой	DoS	2024-02-22	✓

14	Критическая	CVE-2024-0057	Tenable Identity Exposure	Сетевой	SB	2024-02-22	✓

1

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric Electrical Discharge Machines

Идентификатор уязвимости: CVE-2023-21554

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Sinker EDM SG28: все версии
Sinker EDM SG12: все версии
Sinker EDM SG8: все версии
Sinker EDM SV12P: все версии
Sinker EDM SV8P: все версии
Wire-cut EDM MX2400: все версии
Wire-cut EDM MX900: все версии
Wire-cut EDM MP4800: все версии
Wire-cut EDM MP2400: все версии
Wire-cut EDM MP1200: все версии
Wire-cut EDM MV4800R: все версии
Wire-cut EDM MV2400R: все версии
Wire-cut EDM MV1200R: все версии
Wire-cut EDM MV4800S: все версии
Wire-cut EDM MV2400S: все версии
Wire-cut EDM MV1200S: все версии

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-051-03
- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-022_en.pdf
- https://bdu.fstec.ru/vul/2023-02235

2

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1672

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.128

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1672

3

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-26192

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.128

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26192

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

Идентификатор уязвимости: CVE-2024-1595

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: CNCSoft-B: 1.0.0.4
Delta Industrial Automation DOPSoft: до 4.0.0.82

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

4

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: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-053-01

Краткое описание: Получение конфиденциальной информации в Commend WS203VICM

Идентификатор уязвимости: CVE-2024-21767

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: WS203VICM: 1.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-051-01

6

Краткое описание: Отказ в обслуживании в Commend WS203VICM

Идентификатор уязвимости: CVE-2024-22182

Идентификатор программной ошибки: CWE-88 Внедрение или изменение аргументов

Уязвимый продукт: WS203VICM: 1.7

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:U/C:L/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-051-01

Краткое описание: Выполнение произвольного кода в LibTIFF

Идентификатор уязвимости: CVE-2023-52356

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LibTIFF: 4.0 - 4.6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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.

7

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: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2023-52356
- http://bugzilla.redhat.com/show_bug.cgi?id=2251344
- http://gitlab.com/libtiff/libtiff/-/issues/622
- http://gitlab.com/libtiff/libtiff/-/merge_requests/546
- https://bdu.fstec.ru/vul/2024-00967

8

Краткое описание: Выполнение произвольного кода в LibTIFF

Идентификатор уязвимости: CVE-2023-52355

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: LibTIFF: 4.0 - 4.6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 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: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2023-52355
- http://bugzilla.redhat.com/show_bug.cgi?id=2251326
- http://gitlab.com/libtiff/libtiff/-/issues/621
- https://bdu.fstec.ru/vul/2024-01246

Краткое описание: Выполнение произвольного кода в LibTIFF

Идентификатор уязвимости: CVE-2023-6228

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

Уязвимый продукт: LibTIFF: 4.0 - 4.6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 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: 2024-02-23 / 2024-02-23

Ссылки на источник:

- http://bugzilla.redhat.com/show_bug.cgi?id=2240995
- http://gitlab.com/libtiff/libtiff/-/issues/606
- https://bdu.fstec.ru/vul/2024-01277

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-6817

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Chrome OS: до 120.0.6099.294

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

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-22 / 2024-02-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_21.html

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-0611

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Chrome OS: до 120.0.6099.294

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

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-22 / 2024-02-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_21.html

12

Краткое описание: Повышение привилегий в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-0646

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 120.0.6099.294

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-22 / 2024-02-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_21.html
- https://bdu.fstec.ru/vul/2024-00674

13

Краткое описание: Отказ в обслуживании в Tenable Identity Exposure

Идентификатор уязвимости: CVE-2024-20672

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Tenable Identity Exposure (formerly Tenable.ad): 3.11.3 - 3.59.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 2024-02-22 / 2024-02-22

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-04
- https://bdu.fstec.ru/vul/2024-00337

14

Краткое описание: Обход безопасности в Tenable Identity Exposure

Идентификатор уязвимости: CVE-2024-0057

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Tenable Identity Exposure (formerly Tenable.ad): 3.11.3 - 3.59.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-02-22 / 2024-02-22

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-04
- https://bdu.fstec.ru/vul/2024-00402