НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-04-08.1 | 8 апреля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-20348	Cisco Nexus Dashboard Fabric Controller	Сетевой	RLF	2024-04-04	✓
2	Высокая	CVE-2024-23139	Autodesk FBX Review	Сетевой	ACE	2024-04-03	✓
3	Высокая	CVE-2024-3159	Google Chrome	Сетевой	ACE	2024-04-03	✓
4	Высокая	CVE-2024-3158	Google Chrome	Сетевой	ACE	2024-04-03	✓
5	Высокая	CVE-2024-3156	Google Chrome	Сетевой	OSI	2024-04-03	✓
6	Высокая	CVE-2024-22246	VMware SD-WAN Edge	Сетевой	ACE	2024-04-02	✓
7	Высокая	CVE-2024-28099	KEYENCE CORPORATION VT STUDIO	Сетевой	ACE	2024-04-02	✓
8	Высокая	CVE-2024-29218	KEYENCE KV STUDIO and KV REPLAY VIEWER	Сетевой	ACE	2024-04-02	✓
9	Критическая	CVE-2024-3094	XZ Utils	Сетевой	ACE	2024-04-01	✗

1

Краткое описание: Чтение локальных файлов в Cisco Nexus Dashboard Fabric Controller

Идентификатор уязвимости: CVE-2024-20348

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

Уязвимый продукт: Cisco Nexus Dashboard Fabric Controller (NDFC): 12.1.3

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-04 / 2024-04-04

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-dir-trav-SSn3AYDw

2

Краткое описание: Выполнение произвольного кода в Autodesk FBX Review

Идентификатор уязвимости: CVE-2024-23139

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FBX Review: 1.5.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2024-04-03 / 2024-04-03

Ссылки на источник:

- http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0005
- http://www.zerodayinitiative.com/advisories/ZDI-24-295/

3

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3159

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.87

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-03 / 2024-04-03

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html
- http://crbug.com/330760873

4

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3158

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.87

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-03 / 2024-04-03

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html
- http://crbug.com/329965696

5

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-3156

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.87

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.5 AV:N/AC:H/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: 2024-04-03 / 2024-04-03

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html
- http://crbug.com/329130358

Краткое описание: Выполнение произвольного кода в VMware SD-WAN Edge

Идентификатор уязвимости: CVE-2024-22246

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

Уязвимый продукт: SD-WAN Edge: до 5.0.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-02 / 2024-04-02

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0008.html
- https://bdu.fstec.ru/vul/2024-02569

Краткое описание: Выполнение произвольного кода в KEYENCE CORPORATION VT STUDIO

Идентификатор уязвимости: CVE-2024-28099

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: VT STUDIO: 8.32

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

7 **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: 2024-04-02 / 2024-04-02

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU92825069/index.html

Краткое описание: Выполнение произвольного кода в KEYENCE KV STUDIO and KV REPLAY VIEWER

Идентификатор уязвимости: CVE-2024-29218

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: KV STUDIO: 11.64
KV REPLAY VIEWER: 2.64

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

8

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: 2024-04-02 / 2024-04-02

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU95439120/index.html

Краткое описание: Выполнение произвольного кода в XZ Utils

Идентификатор уязвимости: CVE-2024-3094

Идентификатор программной ошибки: CWE-506 Внедренный вредоносный код

Уязвимый продукт: XZ Utils: 5.6.0 - 5.6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Наличие встроенной вредоносной функциональности в коде приложения

Последствия эксплуатации: Выполнение произвольного кода

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

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

9 **Дата выявления / Дата обновления:** 2024-04-01 / 2024-04-01

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2024-3094
- http://bugzilla.redhat.com/show_bug.cgi?id=2272210
- http://www.openwall.com/lists/oss-security/2024/03/29/4
- http://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
- http://news.ycombinator.com/item?id=39865810
- http://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/
- http://www.theregister.com/2024/03/29/malicious_backdoor_xz/
- http://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094
- http://www.darkreading.com/vulnerabilities-threats/are-you-affected-by-the-backdoor-in-xz-utils
- http://aws.amazon.com/security/security-bulletins/AWS-2024-002/
- http://www.tenable.com/blog/frequently-asked-questions-cve-2024-3094-supply-chain-backdoor-in-xz-utils
- http://openssf.org/blog/2024/03/30/xz-backdoor-cve-2024-3094/
- http://bugzilla.suse.com/show_bug.cgi?id=1222124
- http://security.archlinux.org/CVE-2024-3094

- http://security.alpinelinux.org/vuln/CVE-2024-3094
- http://security-tracker.debian.org/tracker/CVE-2024-3094
- http://lists.freebsd.org/archives/freebsd-security/2024-March/000248.html
- http://news.ycombinator.com/item?id=39877267
- http://gynvael.coldwind.pl/?lang=en&id=782
- https://bdu.fstec.ru/vul/2024-02406