НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-03-20.1 | 20 марта 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-5528	Kubernetes	Сетевой	PE	2023-11-20	✓
2	Высокая	CVE-2024-23334	aiohttp	Сетевой	RLF	2024-01-30	✓
3	Высокая	CVE-2024-1086	Google ChromeOS	Локальный	ACE	2024-03-20	✓
4	Высокая	CVE-2024-1672	Google ChromeOS	Сетевой	OSI	2024-03-20	✓
5	Высокая	CVE-2024-6040	Google ChromeOS	Локальный	PE	2024-03-20	✓
6	Критическая	CVE-2024-0204	Google ChromeOS	Сетевой	OSI	2024-03-20	✓
7	Высокая	CVE-2024-0743	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
8	Высокая	CVE-2024-2615	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
9	Высокая	CVE-2024-2614	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
10	Высокая	CVE-2024-2612	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
11	Высокая	CVE-2024-2608	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
12	Высокая	CVE-2024-2607	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
13	Высокая	CVE-2024-2606	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓

14	Высокая	CVE-2024-2605	Mozilla Firefox	Сетевой	ACE	2024-03-19	✓
15	Высокая	CVE-2024-2630	Google Chrome	Сетевой	OSI	2024-03-19	✓
16	Высокая	CVE-2024-2628	Google Chrome	Сетевой	OSI	2024-03-19	✓
17	Критическая	CVE-2024-28353	TRENDnet TEW-827DRU	Сетевой	ACE	2024-03-19	✗
18	Критическая	CVE-2024-28354	TRENDnet TEW-827DRU	Сетевой	ACE	2024-03-19	✗
19	Высокая	CVE-2024-1753	buildah	Локальный	PE	2024-03-19	✓

1

Краткое описание: Повышение привилегий в Kubernetes

Идентификатор уязвимости: CVE-2023-5528

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

Уязвимый продукт: Kubernetes: 1.8.0 - 1.28.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

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: 7.5 AV:N/AC:H/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: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://github.com/kubernetes/kubernetes/issues/121879
- http://groups.google.com/g/kubernetes-security-announce/c/SL_d4NR8pzA

2

Краткое описание: Чтение локальных файлов в aiohttp

Идентификатор уязвимости: CVE-2024-23334

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

Уязвимый продукт: aiohttp: 1.0.5 - 3.9.1

Категория уязвимого продукта: Прикладное программное обеспечение

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/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-30 / 2024-01-30

Ссылки на источник:

- http://github.com/aio-libs/aiohttp/security/advisories/GHSA-5h86-8mv2-jq9f
- http://github.com/aio-libs/aiohttp/pull/8079
- http://github.com/aio-libs/aiohttp/commit/1c335944d6a8b1298baf179b7c0b3069f10c514b
- https://bdu.fstec.ru/vul/2024-00995

3

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-1086

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 120.0.6099.302

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

Способ эксплуатации: Не определено

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: 2024-03-20 / 2024-03-20

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/long-term-support-channel-update-for_19.html
- https://bdu.fstec.ru/vul/2024-01187

4

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-1672

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

Уязвимый продукт: Chrome OS: до 120.0.6099.302

Категория уязвимого продукта: Unix-подобные операционные системы 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: 2024-03-20 / 2024-03-20

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/long-term-support-channel-update-for_19.html
- https://bdu.fstec.ru/vul/2024-01584

Краткое описание: Повышение привилегий в Google ChromeOS

Идентификатор уязвимости: CVE-2024-6040

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Chrome OS: до 120.0.6099.301

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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: 7.8 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: 2024-03-20 / 2024-03-20

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/long-term-support-channel-update-for_11.html

6

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-0204

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Chrome OS: до 120.0.6099.301

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

Способ эксплуатации: Обход ограничений безопасности

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: 9.8 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: 2024-03-20 / 2024-03-20

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/long-term-support-channel-update-for_11.html
- https://bdu.fstec.ru/vul/2024-00665

7

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-0743

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: Firefox ESR: 115.0.1 - 115.8.0

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/
- https://bdu.fstec.ru/vul/2024-00804

8

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2615

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

Уязвимый продукт: Mozilla Firefox: 116.0 - 123.0.1
Firefox for Android: 116.0 - 123.1.0

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2614

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 123.0.1
Firefox ESR: 102.0 - 115.8.0
Firefox for Android: 100.1.0 - 123.1.0

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2612

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 123.0.1
Firefox ESR: 102.0 - 115.8.0
Firefox for Android: 100.1.0 - 123.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2608

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 123.0.1
Firefox ESR: 102.0 - 115.8.0
Firefox for Android: 100.1.0 - 123.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2607

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 123.0.1
Firefox ESR: 102.0 - 115.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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: 7.5 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2606

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Mozilla Firefox: 116.0 - 123.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-2605

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Mozilla Firefox: 100.0 - 123.0.1
Firefox ESR: 102.0 - 115.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

14 **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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

15

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-2630

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 122.0.6261.129

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html
- http://crbug.com/41481877

16

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-2628

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 122.0.6261.129

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: 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: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html
- http://crbug.com/41487774

17

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-827DRU

Идентификатор уязвимости: CVE-2024-28353

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

Уязвимый продукт: TEW-827DRU: 2.10B01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://warp-desk-89d.notion.site/TEW-827DRU-5c40fb20572148f0b00f329d69273791

18

Краткое описание: Выполнение произвольного кода в TRENDnet TEW-827DRU

Идентификатор уязвимости: CVE-2024-28354

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

Уязвимый продукт: TEW-827DRU: 2.10B01

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://warp-desk-89d.notion.site/TEW-827DRU-c732df50b2454ecaa5451b02f3adda6a

19

Краткое описание: Повышение привилегий в buildah

Идентификатор уязвимости: CVE-2024-1753

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: buildah: 1.35.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-19 / 2024-03-19

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2024-1753
- http://bugzilla.redhat.com/show_bug.cgi?id=2265513
- http://github.com/containers/buildah/security/advisories/GHSA-pmf3-c36m-g5cf
- http://github.com/containers/podman/security/advisories/GHSA-874v-pj72-92f3