НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-02-05.1 | 5 февраля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-23653	BuildKit	Сетевой	PE	2024-02-02	✓
2	Критическая	CVE-2024-23652	BuildKit	Сетевой	RLF	2024-02-02	✓
3	Высокая	CVE-2024-23651	BuildKit	Сетевой	OSI	2024-02-02	✓
4	Высокая	CVE-2024-21626	BuildKit	Локальный	OSI	2024-02-02	✓
5	Высокая	CVE-2024-1077	Microsoft Edge	Сетевой	ACE	2024-02-02	✓
6	Высокая	CVE-2024-1060	Microsoft Edge	Сетевой	ACE	2024-02-02	✓
7	Высокая	CVE-2024-1059	Microsoft Edge	Сетевой	ACE	2024-02-02	✓
8	Высокая	CVE-2024-21399	Microsoft Edge	Сетевой	ACE	2024-02-02	✓

1

Краткое описание: Повышение привилегий в BuildKit

Идентификатор уязвимости: CVE-2024-23653

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: BuildKit: 0.3.0 - 0.12.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Ссылки на источник:

- http://github.com/moby/buildkit/security/advisories/GHSA-wr6v-9f75-vh2g
- http://github.com/moby/buildkit/pull/4602
- http://github.com/moby/buildkit/releases/tag/v0.12.5

2

Краткое описание: Чтение локальных файлов в BuildKit

Идентификатор уязвимости: CVE-2024-23652

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

Уязвимый продукт: BuildKit: 0.3.0 - 0.12.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://github.com/moby/buildkit/security/advisories/GHSA-4v98-7qmw-rqr8
- http://github.com/moby/buildkit/pull/4603
- http://github.com/moby/buildkit/releases/tag/v0.12.5

3

Краткое описание: Получение конфиденциальной информации в BuildKit

Идентификатор уязвимости: CVE-2024-23651

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: BuildKit: 0.3.0 - 0.12.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://github.com/moby/buildkit/security/advisories/GHSA-m3r6-h7wv-7xxv
- http://github.com/moby/buildkit/pull/4604
- http://github.com/moby/buildkit/releases/tag/v0.12.5

4

Краткое описание: Получение конфиденциальной информации в BuildKit

Идентификатор уязвимости: CVE-2024-21626

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: BuildKit: 0.3.0 - 0.12.4

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

Ссылки на источник:

- http://github.com/moby/buildkit/releases/tag/v0.12.5

5

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1077

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.83

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1077

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1060

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.83

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1060

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-1059

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.83

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1059

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-21399

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 121.0.2277.83

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399