НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-05-10.1 | 10 мая 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-30986	Solid Edge SE2023	Локальный	ACE	2023-05-10	✓
2	Высокая	CVE-2023-0464	OpenSSL	Сетевой	DoS	2023-05-10	✓
3	Высокая	CVE-2023-2461	Chrome OS	Сетевой	OSI	2023-05-10	✓
4	Высокая	CVE-2023-24903	Windows	Сетевой	ACE	2023-05-09	✓
5	Высокая	CVE-2023-24940	Windows	Сетевой	DoS	2023-05-09	✓
6	Критическая	CVE-2023-24943	Windows	Сетевой	ACE	2023-05-09	✓
7	Высокая	CVE-2023-29325	Windows	Сетевой	ACE	2023-05-09	✓
8	Высокая	CVE-2023-29336	Windows	Локальный	ACE	2023-05-09	✓
9	Высокая	CVE-2023-24953	Microsoft Office	Локальный	ACE	2023-05-09	✓
10	Высокая	CVE-2023-29341	AV1 Video Extension	Локальный	ACE	2023-05-09	✓
11	Высокая	CVE-2023-29340	AV1 Video Extension	Локальный	ACE	2023-05-09	✓
12	Высокая	CVE-2023-28283	Windows	Сетевой	ACE	2023-05-09	✓
13	Высокая	CVE-2023-32207	Mozilla Firefox	Сетевой	XSS\CSS	2023-05-09	✓

14	Высокая	CVE-2023-32206	Mozilla Firefox	Сетевой	DoS	2023-05-09	✓
15	Высокая	CVE-2023-32205	Mozilla Firefox	Сетевой	XSS\CSS	2023-05-09	✓
16	Высокая	CVE-2023-23969	Red Hat Satellite	Сетевой	DoS	2023-05-08	✓
17	Высокая	CVE-2023-24580	Red Hat Satellite	Сетевой	DoS	2023-05-08	✓
18	Высокая	CVE-2023-0767	Multicluster Engine for Kubernetes	Сетевой	ACE	2023-05-08	✓
19	Высокая	CVE-2023-24998	Red Hat Camel for Spring Boot	Сетевой	DoS	2023-05-08	✓
20	Высокая	CVE-2023-22602	Red Hat Camel for Spring Boot	Сетевой	SB	2023-05-08	✓
21	Высокая	CVE-2023-20860	Red Hat Camel for Spring Boot	Сетевой	SB	2023-05-08	✓
22	Высокая	CVE-2023-1370	Red Hat Camel for Spring Boot	Сетевой	DoS	2023-05-08	✓
23	Высокая	CVE-2023-29350	Microsoft Edge	Сетевой	ACE	2023-05-06	✓
24	Критическая	CVE-2023-2478	Gitlab Community Edition	Сетевой	CI	2023-05-05	✓
25	Критическая	CVE-2022-42889	IBM Cognos Command Center	Сетевой	ACE	2023-05-05	✓

1

Краткое описание: Выполнение произвольного кода в Solid Edge SE2023

Идентификатор уязвимости: CVE-2023-30986

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

Уязвимый продукт: Solid Edge SE2023: до X.223.0 Update 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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-10 / 2023-05-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-932528.pdf

2

Краткое описание: Отказ в обслуживании в OpenSSL

Идентификатор уязвимости: CVE-2023-0464

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

Уязвимый продукт: OpenSSL: от 1.0.2 до 1.0.2zh (OpenSSL)
OpenSSL: от 1.1.1 до 1.1.1u (OpenSSL)
OpenSSL: от 3.0.0 до 3.0.9 (OpenSSL)
OpenSSL: от 3.1.0 до 3.1.1
12 SP3 (SUSE Linux Enterprise Server for SAP Applications)
8.0 (Red Hat Enterprise Linux)
12 SP5 (Suse Linux Enterprise Server)
10 (Debian GNU/Linux)
12 (SUSE Linux Enterprise Server for SAP Applications)
12 SP4-LTSS (Suse Linux Enterprise Server)
15 SP1-LTSS (Suse Linux Enterprise Server)
11 (Debian GNU/Linux)
15 SP2 LTSS (Suse Linux Enterprise Server)
7.3 (РЕД ОС)
15.4 (OpenSUSE Leap)
15 SP4 (Suse Linux Enterprise Server)
9 (Red Hat Enterprise Linux)
4.3 (SUSE Manager Retail Branch Server)
4.3 (SUSE Manager Proxy)
4.3 (SUSE Manager Server)
5.2 (openSUSE Leap Micro)
5.3 (openSUSE Leap Micro)
IBM i: 7.2 - 7.5

Категория уязвимого продукта: Unix-подобные операционные системы и их 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-10 / 2023-05-10

Ссылки на источник:

- http://www.ibm.com/support/pages/node/6989163
- https://bdu.fstec.ru/vul/2023-02108
- https://www.openssl.org/news/secadv/20230322.txt
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- https://www.suse.com/security/cve/CVE-2023-0464.html
- https://access.redhat.com/security/cve/CVE-2023-0464
- https://security-tracker.debian.org/tracker/CVE-2023-0464
- https://nvd.nist.gov/vuln/detail/CVE-2023-0464

3

Краткое описание: Получение конфиденциальной информации в Chrome OS

Идентификатор уязвимости: CVE-2023-2461

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 113.0.5672.114

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-10 / 2023-05-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/05/stable-channel-update-for-chromeos.html

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-24903

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

Уязвимый продукт: Windows: 10 - 10 S, 11 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24903

5

Краткое описание: Отказ в обслуживании в Windows

Идентификатор уязвимости: CVE-2023-24940

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 10 S, 11 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24940

6

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-24943

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 10 S, 11 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24943

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-29325

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

Уязвимый продукт: Windows: 10 - 10 S, 11 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29325

8

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-29336

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

Уязвимый продукт: Windows: 10 - 10 S
Windows Server: 2008 - 2016

Категория уязвимого продукта: Операционные системы Microsoft 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29336

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2023-24953

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office: 2019 - 2019 for Mac
Office Online Server : все версии
Microsoft Excel: 2013 RT Service Pack 1 - 2016
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

9

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24953

10

Краткое описание: Выполнение произвольного кода в AV1 Video Extension

Идентификатор уязвимости: CVE-2023-29341

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: AV1 Video Extension: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29341

11

Краткое описание: Выполнение произвольного кода в AV1 Video Extension

Идентификатор уязвимости: CVE-2023-29340

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: AV1 Video Extension: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29340

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-28283

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

Уязвимый продукт: Windows: 10 - 10 S, 11 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-28283

Краткое описание: Межсайтовый скриптинг в Mozilla Firefox

Идентификатор уязвимости: CVE-2023-32207

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Mozilla Firefox: 100.0 - 112.0.2
Firefox ESR: 102.0 - 102.10.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Межсайтовый скриптинг

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.

13

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-16/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox

Идентификатор уязвимости: CVE-2023-32206

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Firefox: 100.0 - 112.0.2
Firefox ESR: 102.0 - 102.10.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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.

14

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-16/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-17/

Краткое описание: Межсайтовый скриптинг в Mozilla Firefox

Идентификатор уязвимости: CVE-2023-32205

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Mozilla Firefox: 100.0 - 112.0.2
Firefox ESR: 102.0 - 102.10.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Межсайтовый скриптинг

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.

15

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-09 / 2023-05-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-16/
- http://www.mozilla.org/en-US/security/advisories/mfsa2023-17/

16

Краткое описание: Отказ в обслуживании в Red Hat Satellite

Идентификатор уязвимости: CVE-2023-23969

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Red Hat Satellite: до 6.13

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2097
- https://bdu.fstec.ru/vul/2023-00662

17

Краткое описание: Отказ в обслуживании в Red Hat Satellite

Идентификатор уязвимости: CVE-2023-24580

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

Уязвимый продукт: Red Hat Satellite: до 6.13

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2097

18

Краткое описание: Выполнение произвольного кода в Multicluster Engine for Kubernetes

Идентификатор уязвимости: CVE-2023-0767

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Multicluster Engine for Kubernetes: 2.0 - 2.0.7

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2098
- https://bdu.fstec.ru/vul/2023-01270

19

Краткое описание: Отказ в обслуживании в Red Hat Camel for Spring Boot

Идентификатор уязвимости: CVE-2023-24998

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Red Hat Camel for Spring Boot: до 3.20.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2100
- https://bdu.fstec.ru/vul/2023-02037

Краткое описание: Обход безопасности в Red Hat Camel for Spring Boot

Идентификатор уязвимости: CVE-2023-22602

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Red Hat Camel for Spring Boot: до 3.20.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2100

21

Краткое описание: Обход безопасности в Red Hat Camel for Spring Boot

Идентификатор уязвимости: CVE-2023-20860

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Red Hat Camel for Spring Boot: до 3.20.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2100
- https://bdu.fstec.ru/vul/2023-02018

Краткое описание: Отказ в обслуживании в Red Hat Camel for Spring Boot

Идентификатор уязвимости: CVE-2023-1370

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: Red Hat Camel for Spring Boot: до 3.20.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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.

22

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-08 / 2023-05-08

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:2100

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-29350

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 112.0.1722.68

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.

23

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-06 / 2023-05-06

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29350

Краткое описание: Внедрение кода в Gitlab Community Edition

Идентификатор уязвимости: CVE-2023-2478

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

Уязвимый продукт: Gitlab Community Edition: 15.4.0 - 15.11.1
GitLab Enterprise Edition: 15.4.0 - 15.11.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

Последствия эксплуатации: Внедрение 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: 9.6 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-05 / 2023-05-05

Ссылки на источник:

- http://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/

25

Краткое описание: Выполнение произвольного кода в IBM Cognos Command Center

Идентификатор уязвимости: CVE-2022-42889

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: IBM Cognos Command Center: до 10.2.4 Fix Pack 1 IF17

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-05 / 2023-05-05

Ссылки на источник:

- http://www.ibm.com/support/pages/node/6988263
- https://bdu.fstec.ru/vul/2022-06275