НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-04-24.1 | 24 апреля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновление
1	Высокая	CVE-2023-30630	SUSE Linux Enterprise Micro for Rancher	Локальный	PE	2023-04-24	✓
2	Критическая	CVE-2021-38578	SUSE Linux Enterprise Micro for Rancher	Сетевой	PE	2023-04-24	✓
3	Высокая	CVE-2023-27385	CX-Drive	Локальный	ACE	2023-04-24	✗
4	Высокая	CVE-2023-27351	PaperCut NG	Сетевой	ACE	2023-04-24	✓
5	Критическая	CVE-2023-27350	PaperCut NG, PaperCut MF	Сетевой	ACE	2023-04-24	✓
6	Высокая	CVE-2023-28432	minio	Сетевой	OSI	2023-04-24	✓
7	Высокая	CVE-2023-0286	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	DoS	2023-04-22	✓
8	Высокая	CVE-2023-0215	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	DoS	2023-04-22	✓
9	Высокая	CVE-2022-48303	OpenShift Data Foundation (formerly OpenShift Container Storage)	Локальный	ACE	2023-04-22	✓
10	Высокая	CVE-2022-45061	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	DoS	2023-04-22	✓
11	Высокая	CVE-2022-4450	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	DoS	2023-04-22	✓
12	Высокая	CVE-2021-28861	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	OSI	2023-04-22	✓

13	Высокая	CVE-2020-10735	OpenShift Data Foundation (formerly OpenShift Container Storage)	Сетевой	DoS	2023-04-22	✓

1

Краткое описание: Повышение привилегий в SUSE Linux Enterprise Micro for Rancher

Идентификатор уязвимости: CVE-2023-30630

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

Уязвимый продукт: SUSE Linux Enterprise Micro for Rancher: 5.3 - 5.4
SUSE Linux Enterprise Micro: 5.3 - 5.4
SUSE Linux Enterprise Server for SAP Applications 15: SP4
SUSE Linux Enterprise Server 15: SP4
SUSE Linux Enterprise Real Time 15: SP4
SUSE Linux Enterprise High Performance Computing 15: SP4
SUSE Linux Enterprise Desktop 15: SP4
Basesystem Module: 15-SP4
openSUSE Leap Micro: 5.3
SUSE Manager Retail Branch Server: 4.3
SUSE Manager Server: 4.3
SUSE Manager Proxy: 4.3
openSUSE Leap: 15.4
dmidecode: до 3.4-150400.16.8.1
dmidecode-debugsource: до 3.4-150400.16.8.1
dmidecode-debuginfo: до 3.4-150400.16.8.1

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 7.8 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: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20231947-1/

2

Краткое описание: Повышение привилегий в SUSE Linux Enterprise Micro for Rancher

Идентификатор уязвимости: CVE-2021-38578

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: SUSE Linux Enterprise Micro for Rancher: 5.2
SUSE Linux Enterprise Server for SAP Applications 15: SP3
SUSE Linux Enterprise Server 15 SP3 LTSS: 15-SP3
SUSE Linux Enterprise Server 15: SP3
SUSE Linux Enterprise Real Time 15: SP3
SUSE Linux Enterprise High Performance Computing LTSS 15: SP3
SUSE Linux Enterprise High Performance Computing ESPOS 15: SP3
SUSE Linux Enterprise High Performance Computing 15: SP3
SUSE Enterprise Storage: 7.1
SUSE Manager Retail Branch Server: 4.2
SUSE Linux Enterprise Micro: 5.1 - 5.2
SUSE Manager Server: 4.2
SUSE Manager Proxy: 4.2
qemu-uefi-aarch64: до 202008-150300.10.20.1
qemu-ovmf-x86_64: до 202008-150300.10.20.1
ovmf-tools: до 202008-150300.10.20.1
ovmf: до 202008-150300.10.20.1

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20231958-1/

3

Краткое описание: Выполнение произвольного кода в CX-Drive

Идентификатор уязвимости: CVE-2023-27385

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

Уязвимый продукт: CX-Drive: 3.01

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного SDD файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU97372625/index.html
- http://www.ia.omron.com/product/vulnerability/OMSR-2023-004_en.pdf

4

Краткое описание: Выполнение произвольного кода в PaperCut NG

Идентификатор уязвимости: CVE-2023-27351

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: PaperCut NG: до 22.0.9
PaperCut MF: до 22.0.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://www.papercut.com/kb/Main/PO-1216-and-PO-1219
- http://www.zerodayinitiative.com/advisories/ZDI-23-232/

5

Краткое описание: Выполнение произвольного кода в PaperCut NG, PaperCut MF

Идентификатор уязвимости: CVE-2023-27350

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: PaperCut NG, PaperCut MF: до 22.0.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://www.papercut.com/kb/Main/PO-1216-and-PO-1219
- http://www.zerodayinitiative.com/advisories/ZDI-23-233/

Краткое описание: Получение конфиденциальной информации в minio

Идентификатор уязвимости: CVE-2023-28432

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: minio: 2019-12-17T23-16-33Z - 2023-03-13T19-46-17Z

Категория уязвимого продукта: Прикладное программное обеспечение

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.

6

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-24 / 2023-04-24

Ссылки на источник:

- http://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q
- http://github.com/minio/minio/releases/tag/RELEASE.2023-03-20T20-16-18Z
- http://www.greynoise.io/blog/openai-minio-and-why-you-should-always-use-docker-cli-scan-to-keep-your-supply-chain-clean
- http://twitter.com/Andrew__Morris/status/1639325397241278464
- http://viz.greynoise.io/tag/minio-information-disclosure-attempt
- https://bdu.fstec.ru/vul/2023-02098

7

Краткое описание: Отказ в обслуживании в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2023-0286

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816
- https://bdu.fstec.ru/vul/2023-00665

8

Краткое описание: Отказ в обслуживании в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2023-0215

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем 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.

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: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816
- https://bdu.fstec.ru/vul/2023-00675

9

Краткое описание: Выполнение произвольного кода в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2022-48303

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

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

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: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816
- https://bdu.fstec.ru/vul/2023-00577

Краткое описание: Отказ в обслуживании в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2022-45061

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

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

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.

10

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: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816

Краткое описание: Отказ в обслуживании в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2022-4450

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 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: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816

Краткое описание: Получение конфиденциальной информации в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2021-28861

Идентификатор программной ошибки: CWE-601 Перенаправление на небезопасный сайт ("открытое перенаправление")

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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.

12

Оценка CVSSv3: 7.4 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816

13

Краткое описание: Отказ в обслуживании в OpenShift Data Foundation (formerly OpenShift Container Storage)

Идентификатор уязвимости: CVE-2020-10735

Идентификатор программной ошибки: CWE-704 Некорректное преобразование или приведение типов

Уязвимый продукт: OpenShift Data Foundation (formerly OpenShift Container Storage): 4.12 - 4.12.1

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: 2023-04-22 / 2023-04-22

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:1816
- https://bdu.fstec.ru/vul/2022-05599