НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-06-14.1 | 14 июня 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-29011	Visual Studio	Локальный	PE	2023-06-14	✓
2	Высокая	CVE-2023-29366	Windows Server	Локальный	ACE	2023-06-14	✓
3	Высокая	CVE-2023-2953	Development Tools Module	Сетевой	DoS	2023-06-14	✓
4	Высокая	CVE-2023-33146	Microsoft Office	Локальный	ACE	2023-06-14	✓
5	Высокая	CVE-2023-25652	Visual Studio	Сетевой	PE	2023-06-14	✓
6	Высокая	CVE-2023-34290	Cobalt	Локальный	ACE	2023-06-09	✓
7	Высокая	CVE-2023-34289	Cobalt	Локальный	ACE	2023-06-09	✓
8	Высокая	CVE-2023-34287	Cobalt	Локальный	ACE	2023-06-09	✓
9	Высокая	CVE-2023-34286	Cobalt	Локальный	ACE	2023-06-09	✓
10	Высокая	CVE-2018-7208	SUSE Linux Enterprise Software Development Kit 12	Локальный	DoS	2023-06-12	✓
11	Высокая	CVE-2017-16829	SUSE Linux Enterprise Software Development Kit 12	Локальный	DoS	2023-06-12	✓
12	Высокая	CVE-2022-39286	Debian Linux	Сетевой	ACE	2023-06-13	✓
13	Высокая	CVE-2023-2610	Ubuntu	Локальный	ACE	2023-06-13	✓

14	Высокая	CVE-2023-2609	Ubuntu	Локальный	DoS	2023-06-13	✓
15	Критическая	CVE-2023-25076	Ubuntu	Сетевой	ACE	2023-06-13	✓
16	Критическая	CVE-2021-28235	Red Hat OpenStack	Сетевой	OSI	2023-06-06	✓
17	Высокая	CVE-2023-30861	Red Hat OpenStack	Сетевой	OSI	2023-06-06	✓
18	Высокая	CVE-2023-32233	Ubuntu	Локальный	PE	2023-06-09	✓
19	Высокая	CVE-2023-31436	Ubuntu	Локальный	PE	2023-06-09	✓
20	Высокая	CVE-2023-24329	Slackware Linux	Сетевой	SB	2023-06-09	✓
21	Высокая	CVE-2022-27664	Consul Enterprise	Сетевой	DoS	2023-06-08	✓
22	Высокая	CVE-2023-24536	Consul Enterprise	Сетевой	DoS	2023-06-08	✓
23	Высокая	CVE-2022-41723	Consul Enterprise	Сетевой	DoS	2023-06-08	✓

1

Краткое описание: Повышение привилегий в Visual Studio

Идентификатор уязвимости: CVE-2023-29011

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Visual Studio: до 2022 version 17.6.3

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка 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: 7.5 AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-14 / 2023-06-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29011

2

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2023-29366

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: 2019 - 2022 20H2
Windows: 10 - 11 22H2

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: 2023-06-14 / 2023-06-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29366

3

Краткое описание: Отказ в обслуживании в Development Tools Module

Идентификатор уязвимости: CVE-2023-2953

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Development Tools Module: 15-SP4 - 15-SP5
Basesystem Module: 15-SP4 - 15-SP5
SUSE Linux Enterprise Micro for Rancher: 5.2 - 5.4
SUSE Linux Enterprise Server for SAP Applications 15: SP4 - SP5
SUSE Linux Enterprise Server 15: SP4 - SP5
SUSE Linux Enterprise Real Time 15: SP3 - SP5
SUSE Linux Enterprise High Performance Computing 15: SP4 - SP5
SUSE Linux Enterprise Desktop 15: SP4 - SP5
SUSE Linux Enterprise Micro: 5.1 - 5.4
openSUSE Leap: 15.4 - 15.5
openSUSE Leap Micro: 5.3 - 5.3
SUSE Manager Retail Branch Server: 4.3 - 4.3
SUSE Manager Server: 4.3 - 4.3
SUSE Manager Proxy: 4.3 - 4.3
openldap2-doc: до 2.4.46-150200.14.14.1
openldap2-devel-32bit: до 2.4.46-150200.14.14.1
libldap-2_4-2-32bit: до 2.4.46-150200.14.14.1
libldap-2_4-2-32bit-debuginfo: до 2.4.46-150200.14.14.1
openldap2-ppolicy-check-password: до 1.2-150200.14.14.1
openldap2: до 2.4.46-150200.14.14.1
openldap2-back-sql: до 2.4.46-150200.14.14.1
openldap2-devel: до 2.4.46-150200.14.14.1
openldap2-client-debuginfo: до 2.4.46-150200.14.14.1
openldap2-back-sock-debuginfo: до 2.4.46-150200.14.14.1
openldap2-back-perl: до 2.4.46-150200.14.14.1
openldap2-contrib-debuginfo: до 2.4.46-150200.14.14.1
openldap2-back-perl-debuginfo: до 2.4.46-150200.14.14.1
openldap2-back-sock: до 2.4.46-150200.14.14.1
openldap2-contrib: до 2.4.46-150200.14.14.1
openldap2-back-sql-debuginfo: до 2.4.46-150200.14.14.1

openldap2-back-meta: до 2.4.46-150200.14.14.1
openldap2-ppolicy-check-password-debuginfo: до 1.2-150200.14.14.1
openldap2-client: до 2.4.46-150200.14.14.1
openldap2-back-meta-debuginfo: до 2.4.46-150200.14.14.1
openldap2-devel-static: до 2.4.46-150200.14.14.1
libldap-data: до 2.4.46-150200.14.14.1
openldap2-debugsource: до 2.4.46-150200.14.14.1
libldap-2_4-2-debuginfo: до 2.4.46-150200.14.14.1
openldap2-debuginfo: до 2.4.46-150200.14.14.1
libldap-2_4-2: до 2.4.46-150200.14.14.1

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: 2023-06-14 / 2023-06-14

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232484-1/

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2023-33146

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

Уязвимый продукт: Microsoft Office: 2019 - 2019 for Mac
Microsoft Office LTSC 2021: 2021 for Mac - 2021 for Mac
Microsoft 365 Apps for Enterprise: до 2305 16501.20210

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2023-06-14 / 2023-06-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-33146

Краткое описание: Повышение привилегий в Visual Studio

Идентификатор уязвимости: CVE-2023-25652

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Visual Studio: до 2022 version 17.6.3

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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: 7.5 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: 2023-06-14 / 2023-06-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-25652

6

Краткое описание: Выполнение произвольного кода в Cobalt

Идентификатор уязвимости: CVE-2023-34290

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Cobalt: до 12.0.1204.54

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: 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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-828/

7

Краткое описание: Выполнение произвольного кода в Cobalt

Идентификатор уязвимости: CVE-2023-34289

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

Уязвимый продукт: Cobalt: до 12.0.1204.54

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: 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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-827/

8

Краткое описание: Выполнение произвольного кода в Cobalt

Идентификатор уязвимости: CVE-2023-34287

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Cobalt: до 12.0.1204.54

Категория уязвимого продукта: Прикладное программное обеспечение

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: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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-825/

9

Краткое описание: Выполнение произвольного кода в Cobalt

Идентификатор уязвимости: CVE-2023-34286

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Cobalt: до 12.0.1204.54

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: 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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-824/

10

Краткое описание: Отказ в обслуживании в SUSE Linux Enterprise Software Development Kit 12

Идентификатор уязвимости: CVE-2018-7208

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SUSE Linux Enterprise Software Development Kit 12: SP5 - SP5
SUSE Linux Enterprise Server for SAP Applications 12: SP5 - SP5
SUSE Linux Enterprise Server 12: SP5 - SP5
SUSE Linux Enterprise High Performance Computing 12: SP5 - SP5
gdb: до 12.1-2.20.1
gdbserver-32bit: до 12.1-2.20.1
gdbserver-debuginfo-32bit: до 12.1-2.20.1
gdb-debuginfo-32bit: до 12.1-2.20.1
gdbserver-debuginfo: до 12.1-2.20.1
gdbserver: до 12.1-2.20.1
gdb-debugsource: до 12.1-2.20.1
gdb-debuginfo: до 12.1-2.20.1

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 7.8 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: 2023-06-12 / 2023-06-12

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232485-1/

- https://bdu.fstec.ru/vul/2019-00569

11

Краткое описание: Отказ в обслуживании в SUSE Linux Enterprise Software Development Kit 12

Идентификатор уязвимости: CVE-2017-16829

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SUSE Linux Enterprise Software Development Kit 12: SP5 - SP5
SUSE Linux Enterprise Server for SAP Applications 12: SP5 - SP5
SUSE Linux Enterprise Server 12: SP5 - SP5
SUSE Linux Enterprise High Performance Computing 12: SP5 - SP5
gdb: до 12.1-2.20.1
gdbserver-32bit: до 12.1-2.20.1
gdbserver-debuginfo-32bit: до 12.1-2.20.1
gdb-debuginfo-32bit: до 12.1-2.20.1
gdbserver-debuginfo: до 12.1-2.20.1
gdbserver: до 12.1-2.20.1
gdb-debugsource: до 12.1-2.20.1
gdb-debuginfo: до 12.1-2.20.1

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 7.8 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: 2023-06-12 / 2023-06-12

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232485-1/

12

Краткое описание: Выполнение произвольного кода в Debian Linux

Идентификатор уязвимости: CVE-2022-39286

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Debian Linux: все версии
jupyter-core (Debian package): до 4.7.1-1+deb11u1

Категория уязвимого продукта: Unix-подобные операционные системы 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: 8.8 AV:N/AC:L/PR:L/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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5422

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-2610

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

Уязвимый продукт: Ubuntu: 14.04 - 23.04
vim-tiny (Ubuntu package): до Ubuntu Pro (Infra-only)
vim (Ubuntu package): до Ubuntu Pro (Infra-only)

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6154-1

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2023-2609

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Ubuntu: 14.04 - 23.04
vim-tiny (Ubuntu package): до Ubuntu Pro (Infra-only)
vim (Ubuntu package): до Ubuntu Pro (Infra-only)

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6154-1

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-25076

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

Уязвимый продукт: Ubuntu: 18.04 - 23.04
sniproxy (Ubuntu package): до Ubuntu Pro

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

15 **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: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6148-1

16

Краткое описание: Получение конфиденциальной информации в Red Hat OpenStack

Идентификатор уязвимости: CVE-2021-28235

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Red Hat OpenStack: 17.0 - 17.0
etcd (Red Hat package): до 3.4.26-1.el9ost

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

Способ эксплуатации: Обход процесса авторизации

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

Средства устранения уязвимости: Не определено

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

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:3441

Краткое описание: Получение конфиденциальной информации в Red Hat OpenStack

Идентификатор уязвимости: CVE-2023-30861

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

Уязвимый продукт: Red Hat OpenStack: 17.0 - 17.0
python-flask (Red Hat package): до 1.1.2-6.el9ost

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

17 **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

Средства устранения уязвимости: Не определено

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

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:3440
- https://bdu.fstec.ru/vul/2023-02381

Краткое описание: Повышение привилегий в Ubuntu

Идентификатор уязвимости: CVE-2023-32233

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Ubuntu: 20.04 - 22.04
linux-image-raspi2 (Ubuntu package): до 5.4.0.1086.116
linux-image-5.4.0-1086-raspi (Ubuntu package): до 5.4.0-1086.97
linux-image-5.15.0-1030-raspi-nolpae (Ubuntu package): до 5.15.0-1030.32
linux-image-5.15.0-1031-intel-iotg (Ubuntu package): до 5.15.0-1031.36
linux-image-raspi (Ubuntu package): до 5.15.0.1030.27
linux-image-raspi-nolpae (Ubuntu package): до 5.15.0.1030.27
linux-image-intel-iotg (Ubuntu package): до 5.15.0.1031.30
linux-image-5.15.0-1030-raspi (Ubuntu package): до 5.15.0-1030.32

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

18 **Способ эксплуатации:** Отправка специально сформированного запроса.

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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6150-1
- https://bdu.fstec.ru/vul/2023-02625

Краткое описание: Повышение привилегий в Ubuntu

Идентификатор уязвимости: CVE-2023-31436

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Ubuntu: 20.04 - 22.04
linux-image-raspi2 (Ubuntu package): до 5.4.0.1086.116
linux-image-5.4.0-1086-raspi (Ubuntu package): до 5.4.0-1086.97
linux-image-5.15.0-1030-raspi-nolpae (Ubuntu package): до 5.15.0-1030.32
linux-image-5.15.0-1031-intel-iotg (Ubuntu package): до 5.15.0-1031.36
linux-image-raspi (Ubuntu package): до 5.15.0.1030.27
linux-image-raspi-nolpae (Ubuntu package): до 5.15.0.1030.27
linux-image-intel-iotg (Ubuntu package): до 5.15.0.1031.30
linux-image-5.15.0-1030-raspi (Ubuntu package): до 5.15.0-1030.32

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

19 **Способ эксплуатации:** Отправка специально сформированных данных.

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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6150-1
- https://bdu.fstec.ru/vul/2023-02605

20

Краткое описание: Обход безопасности в Slackware Linux

Идентификатор уязвимости: CVE-2023-24329

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Slackware Linux: 15.0 - 15.0
python3: до 3.9.17

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

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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: 2023-06-09 / 2023-06-09

Ссылки на источник:

- http://www.slackware.com/security/viewer.php?l=slackware-security&y=2023&m=slackware-security.348167

Краткое описание: Отказ в обслуживании в Consul Enterprise

Идентификатор уязвимости: CVE-2022-27664

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Consul Enterprise: 1.13.0 - 1.15.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

21 **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: 2023-06-08 / 2023-06-08

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.13.8
- http://github.com/hashicorp/consul/releases/tag/v1.14.7
- https://bdu.fstec.ru/vul/2022-05544

22

Краткое описание: Отказ в обслуживании в Consul Enterprise

Идентификатор уязвимости: CVE-2023-24536

Идентификатор программной ошибки: CWE-399 Уязвимости, связанные с управлением ресурсами

Уязвимый продукт: Consul Enterprise: 1.13.0 - 1.15.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 2023-06-08 / 2023-06-08

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.13.8
- http://github.com/hashicorp/consul/releases/tag/v1.14.7

23

Краткое описание: Отказ в обслуживании в Consul Enterprise

Идентификатор уязвимости: CVE-2022-41723

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

Уязвимый продукт: Consul Enterprise: 1.13.0 - 1.15.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2023-06-08 / 2023-06-08

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.13.8
- http://github.com/hashicorp/consul/releases/tag/v1.14.7