НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-04-26.1 | 26 апреля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2022-48468	SUSE Linux Enterprise Server for SAP Applications 15	Сетевой	ACE	2023-04-25	✓
2	Критическая	CVE-2023-24538	Ubuntu	Сетевой	ACE	2023-04-25	✓
3	Высокая	CVE-2022-2879	Ubuntu	Сетевой	DoS	2023-04-25	✓
4	Высокая	CVE-2022-27664	Ubuntu	Сетевой	DoS	2023-04-25	✓
5	Высокая	CVE-2023-29011	Git for Windows	Локальный	PE	2023-04-25	✓
6	Высокая	CVE-2023-25652	Git for Windows	Сетевой	PE	2023-04-25	✓
7	Высокая	CVE-2023-20872	VMware Workstation	Локальный	ACE	2023-04-25	✓
8	Критическая	CVE-2023-20869	VMware Workstation	Локальный	ACE	2023-04-25	✓
9	Критическая	CVE-2023-25725	Oracle Linux	Сетевой	OSI	2023-04-24	✓
10	Высокая	CVE-2023-1281	SUSE Linux Enterprise Micro for Rancher	Локальный	PE	2023-04-25	✓
11	Высокая	CVE-2022-4744	SUSE Linux Enterprise Micro for Rancher	Локальный	PE	2023-04-25	✓
12	Критическая	CVE-2023-28771	ATP series	Сетевой	ACE	2023-04-25	✓
13	Высокая	CVE-2023-27991	ATP series	Сетевой	ACE	2023-04-25	✓

Краткое описание: Выполнение произвольного кода в SUSE Linux Enterprise Server for SAP Applications 15

Идентификатор уязвимости: CVE-2022-48468

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

Уязвимый продукт: SUSE Linux Enterprise Server for SAP Applications 15: SP1
SUSE Linux Enterprise Server 15 SP1 LTSS: 15-SP1
SUSE Linux Enterprise Server 15: SP1
SUSE Linux Enterprise High Performance Computing 15 SP1 LTSS: 15-SP1
SUSE Linux Enterprise High Performance Computing 15: SP1
SUSE CaaS Platform: 4.0
libprotobuf-c1-debuginfo: до 1.3.0-150000.3.3.1
libprotobuf-c-devel: до 1.3.0-150000.3.3.1
protobuf-c-debugsource: до 1.3.0-150000.3.3.1
libprotobuf-c1: до 1.3.0-150000.3.3.1
protobuf-c-debuginfo: до 1.3.0-150000.3.3.1

1

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: 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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20231979-1/

2

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-24538

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

Уязвимый продукт: Ubuntu: 22.04, 20.04, 18.04
golang-1.18 (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-src (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-go (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4

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: 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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6038-1

3

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2022-2879

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

Уязвимый продукт: Ubuntu: 22.04, 20.04, 18.04
golang-1.18 (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-src (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-go (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4

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

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.

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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6038-1

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2022-27664

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Ubuntu: 22.04, 20.04, 18.04
golang-1.18 (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-src (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4
golang-1.18-go (Ubuntu package): до 1.18.1-1ubuntu1~18.04.4

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6038-1
- https://bdu.fstec.ru/vul/2022-05544

5

Краткое описание: Повышение привилегий в Git for Windows

Идентификатор уязвимости: CVE-2023-29011

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Git for Windows: 2.40.0 - 2.40.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://github.com/git-for-windows/git/releases/tag/v2.40.1.windows.1
- http://github.com/git-for-windows/git/security/advisories/GHSA-g4fv-xjqw-q7jm

6

Краткое описание: Повышение привилегий в Git for Windows

Идентификатор уязвимости: CVE-2023-25652

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

Уязвимый продукт: Git for Windows: 2.0.0 - 2.40.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://github.com/git-for-windows/git/releases/tag/v2.39.3.windows.1
- http://github.com/git-for-windows/git/releases/tag/v2.40.1.windows.1

Краткое описание: Выполнение произвольного кода в VMware Workstation

Идентификатор уязвимости: CVE-2023-20872

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware Workstation: 17.0 - 17.0.1
VMware Fusion: 13.0 - 13.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.7 AV:L/AC:H/PR:N/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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0008.html

8

Краткое описание: Выполнение произвольного кода в VMware Workstation

Идентификатор уязвимости: CVE-2023-20869

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: VMware Workstation: 17.0 - 17.0.1
VMware Fusion: 13.0 - 13.0.1

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0008.html

9

Краткое описание: Получение конфиденциальной информации в Oracle Linux

Идентификатор уязвимости: CVE-2023-25725

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Oracle Linux: все версии

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

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/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.oracle.com/security-alerts/linuxbulletinapr2023.html
- https://bdu.fstec.ru/vul/2023-00758

10

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

Идентификатор уязвимости: CVE-2023-1281

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SUSE Linux Enterprise Micro for Rancher: 5.3 - 5.4
SUSE Real Time Module: 15-SP4
SUSE Linux Enterprise Micro: 5.3 - 5.4
SUSE Linux Enterprise Live Patching: 15-SP4
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
openSUSE Leap Micro: 5.3
openSUSE Leap: 15.4
kernel-livepatch-SLE15-SP4-RT_Update_6-debugsource: до 1-150400.1.3.3
kernel-livepatch-5_14_21-150400_15_23-rt-debuginfo: до 1-150400.1.3.3
kernel-livepatch-5_14_21-150400_15_23-rt: до 1-150400.1.3.3
kernel-rt_debug: до 5.14.21-150400.15.23.1
kernel-source-rt: до 5.14.21-150400.15.23.1
kernel-devel-rt: до 5.14.21-150400.15.23.1
kernel-rt_debug-devel: до 5.14.21-150400.15.23.1
kernel-rt-devel-debuginfo: до 5.14.21-150400.15.23.1
gfs2-kmp-rt: до 5.14.21-150400.15.23.1
kernel-rt_debug-devel-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt_debug-debugsource: до 5.14.21-150400.15.23.1
gfs2-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
kernel-syms-rt: до 5.14.21-150400.15.23.1
dlm-kmp-rt: до 5.14.21-150400.15.23.1
ocfs2-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
ocfs2-kmp-rt: до 5.14.21-150400.15.23.1
cluster-md-kmp-rt: до 5.14.21-150400.15.23.1
kernel-rt-devel: до 5.14.21-150400.15.23.1
dlm-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
cluster-md-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1

kernel-rt_debug-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt-debugsource: до 5.14.21-150400.15.23.1
kernel-rt: до 5.14.21-150400.15.23.1

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

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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20231992-1/
- https://bdu.fstec.ru/vul/2023-01571

11

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

Идентификатор уязвимости: CVE-2022-4744

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: SUSE Linux Enterprise Micro for Rancher: 5.3 - 5.4
SUSE Real Time Module: 15-SP4
SUSE Linux Enterprise Micro: 5.3 - 5.4
SUSE Linux Enterprise Live Patching: 15-SP4
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
openSUSE Leap Micro: 5.3
openSUSE Leap: 15.4
kernel-livepatch-SLE15-SP4-RT_Update_6-debugsource: до 1-150400.1.3.3
kernel-livepatch-5_14_21-150400_15_23-rt-debuginfo: до 1-150400.1.3.3
kernel-livepatch-5_14_21-150400_15_23-rt: до 1-150400.1.3.3
kernel-rt_debug: до 5.14.21-150400.15.23.1
kernel-source-rt: до 5.14.21-150400.15.23.1
kernel-devel-rt: до 5.14.21-150400.15.23.1
kernel-rt_debug-devel: до 5.14.21-150400.15.23.1
kernel-rt-devel-debuginfo: до 5.14.21-150400.15.23.1
gfs2-kmp-rt: до 5.14.21-150400.15.23.1
kernel-rt_debug-devel-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt_debug-debugsource: до 5.14.21-150400.15.23.1
gfs2-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
kernel-syms-rt: до 5.14.21-150400.15.23.1
dlm-kmp-rt: до 5.14.21-150400.15.23.1
ocfs2-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
ocfs2-kmp-rt: до 5.14.21-150400.15.23.1
cluster-md-kmp-rt: до 5.14.21-150400.15.23.1
kernel-rt-devel: до 5.14.21-150400.15.23.1
dlm-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1
cluster-md-kmp-rt-debuginfo: до 5.14.21-150400.15.23.1

kernel-rt_debug-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt-debuginfo: до 5.14.21-150400.15.23.1
kernel-rt-debugsource: до 5.14.21-150400.15.23.1
kernel-rt: до 5.14.21-150400.15.23.1

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

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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20231992-1/
- https://bdu.fstec.ru/vul/2023-01797

Краткое описание: Выполнение произвольного кода в ATP series

Идентификатор уязвимости: CVE-2023-28771

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

Уязвимый продукт: ATP series: 4.60 - 5.35
USG FLEX series: 4.60 - 5.35
VPN series: 4.60 - 5.35
ZyWALL: 4.60 - 4.73
USG series: 4.60 - 4.73

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

12 **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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

Краткое описание: Выполнение произвольного кода в ATP series

Идентификатор уязвимости: CVE-2023-27991

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

Уязвимый продукт: ATP series: 4.32 - 5.35
USG FLEX series: 4.50 - 5.35
USG FLEX 50W: 4.16 - 5.35
USG20W-VPN: 4.16 - 5.35
VPN series: 4.30 - 5.35

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

13

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: 2023-04-25 / 2023-04-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-and-post-authentication-command-injection-vulnerability-in-firewalls