НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-05.1 | 5 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-29491	VMware Tanzu Application Service for VMs	Локальный	ACE	2023-06-30	✓
2	Высокая	CVE-2021-39537	VMware Tanzu Application Service for VMs	Сетевой	ACE	2023-06-30	✓
3	Высокая	CVE-2023-33733	Ubuntu	Локальный	ACE	2023-07-03	✓
4	Высокая	CVE-2023-32763	Desktop Applications Module	Сетевой	ACE	2023-07-04	✓
5	Высокая	CVE-2023-2650	VMware Tanzu Application Service for VMs	Сетевой	DoS	2023-06-30	✓
6	Высокая	CVE-2023-21930	IBM CICS TX Advanced	Сетевой	RLF	2023-07-05	✓
7	Критическая	CVE-2023-27997	FortiOS	Сетевой	ACE	2023-06-13	✓
8	Не определено	CVE-2023-32393	WebKitGTK+	Не определено	ACE	2023-07-03	✗
9	Высокая	CVE-2023-36664	Artifex Ghostscript	Локальный	ACE	2023-07-04	✓

1

Краткое описание: Выполнение произвольного кода в VMware Tanzu Application Service for VMs

Идентификатор уязвимости: CVE-2023-29491

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

Уязвимый продукт: VMware Tanzu Application Service for VMs: все версии
Isolation Segment: все версии
VMware Tanzu Operations Manager: до 3.0.11
Platform Automation Toolkit: до 5.1.2

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: 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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://tanzu.vmware.com/security/usn-6099-1

2

Краткое описание: Выполнение произвольного кода в VMware Tanzu Application Service for VMs

Идентификатор уязвимости: CVE-2021-39537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware Tanzu Application Service for VMs: все версии
Isolation Segment: все версии
VMware Tanzu Operations Manager: до 3.0.11
Platform Automation Toolkit: до 5.1.2

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: 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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://tanzu.vmware.com/security/usn-6099-1

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-33733

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

Уязвимый продукт: Ubuntu: 20.04 - 23.04
python3-reportlab (Ubuntu package): до 3.6.12-1ubuntu0.1

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

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

3 **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: 2023-07-03 / 2023-07-03

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6196-1
- https://bdu.fstec.ru/vul/2023-03106

4

Краткое описание: Выполнение произвольного кода в Desktop Applications Module

Идентификатор уязвимости: CVE-2023-32763

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

Уязвимый продукт: Desktop Applications Module: 15-SP5 - 15-SP5
SUSE Package Hub 15: 15-SP5 - 15-SP5
SUSE Linux Enterprise Server for SAP Applications 15: SP5 - SP5
SUSE Linux Enterprise Server 15: SP5 - SP5
SUSE Linux Enterprise Real Time 15: SP5 - SP5
SUSE Linux Enterprise High Performance Computing 15: SP5 - SP5
SUSE Linux Enterprise Desktop 15: SP5 - SP5
openSUSE Leap: 15.5 - 15.5
qt6-docs-common: до 6.4.2-150500.3.3.1
qt6-base-private-devel: до 6.4.2-150500.3.3.1
qt6-sql-mysql-debuginfo: до 6.4.2-150500.3.3.1
qt6-base-docs-qch: до 6.4.2-150500.3.3.1
qt6-sql-unixODBC-debuginfo: до 6.4.2-150500.3.3.1
qt6-base-examples: до 6.4.2-150500.3.3.1
qt6-test-private-devel: до 6.4.2-150500.3.3.1
qt6-platformtheme-gtk3: до 6.4.2-150500.3.3.1
qt6-printsupport-private-devel: до 6.4.2-150500.3.3.1
qt6-sql-postgresql: до 6.4.2-150500.3.3.1
qt6-xml-private-devel: до 6.4.2-150500.3.3.1
qt6-platformsupport-private-devel: до 6.4.2-150500.3.3.1
qt6-platformtheme-gtk3-debuginfo: до 6.4.2-150500.3.3.1
qt6-networkinformation-glib-debuginfo: до 6.4.2-150500.3.3.1
qt6-platformtheme-xdgdesktopportal: до 6.4.2-150500.3.3.1
qt6-platformtheme-xdgdesktopportal-debuginfo: до 6.4.2-150500.3.3.1
qt6-networkinformation-nm-debuginfo: до 6.4.2-150500.3.3.1
qt6-printsupport-cups: до 6.4.2-150500.3.3.1
qt6-sql-postgresql-debuginfo: до 6.4.2-150500.3.3.1
qt6-sql-private-devel: до 6.4.2-150500.3.3.1
qt6-network-private-devel: до 6.4.2-150500.3.3.1
qt6-networkinformation-glib: до 6.4.2-150500.3.3.1

qt6-dbus-private-devel: до 6.4.2-150500.3.3.1
qt6-base-examples-debuginfo: до 6.4.2-150500.3.3.1
qt6-sql-unixODBC: до 6.4.2-150500.3.3.1
qt6-sql-mysql: до 6.4.2-150500.3.3.1
qt6-printsupport-cups-debuginfo: до 6.4.2-150500.3.3.1
qt6-networkinformation-nm: до 6.4.2-150500.3.3.1
qt6-base-docs-html: до 6.4.2-150500.3.3.1
qt6-base-devel: до 6.4.2-150500.3.3.1
qt6-network-devel: до 6.4.2-150500.3.3.1
qt6-opengl-devel: до 6.4.2-150500.3.3.1
libQt6PrintSupport6: до 6.4.2-150500.3.3.1
qt6-core-devel: до 6.4.2-150500.3.3.1
qt6-base-common-devel-debuginfo: до 6.4.2-150500.3.3.1
qt6-opengl-private-devel: до 6.4.2-150500.3.3.1
qt6-concurrent-devel: до 6.4.2-150500.3.3.1
libQt6Sql6: до 6.4.2-150500.3.3.1
qt6-widgets-private-devel: до 6.4.2-150500.3.3.1
qt6-sql-devel: до 6.4.2-150500.3.3.1
qt6-widgets-devel: до 6.4.2-150500.3.3.1
qt6-platformsupport-devel-static: до 6.4.2-150500.3.3.1
qt6-core-private-devel: до 6.4.2-150500.3.3.1
qt6-gui-private-devel: до 6.4.2-150500.3.3.1
libQt6OpenGLWidgets6: до 6.4.2-150500.3.3.1
qt6-printsupport-devel: до 6.4.2-150500.3.3.1
qt6-kmssupport-devel-static: до 6.4.2-150500.3.3.1
qt6-openglwidgets-devel: до 6.4.2-150500.3.3.1
qt6-sql-sqlite: до 6.4.2-150500.3.3.1
qt6-dbus-devel: до 6.4.2-150500.3.3.1
qt6-xml-devel: до 6.4.2-150500.3.3.1
qt6-test-devel: до 6.4.2-150500.3.3.1
qt6-gui-devel: до 6.4.2-150500.3.3.1
libQt6Test6-debuginfo: до 6.4.2-150500.3.3.1
libQt6OpenGLWidgets6-debuginfo: до 6.4.2-150500.3.3.1
libQt6Xml6-debuginfo: до 6.4.2-150500.3.3.1

libQt6PrintSupport6-debuginfo: до 6.4.2-150500.3.3.1
libQt6Xml6: до 6.4.2-150500.3.3.1
libQt6Concurrent6: до 6.4.2-150500.3.3.1
libQt6Sql6-debuginfo: до 6.4.2-150500.3.3.1
libQt6Test6: до 6.4.2-150500.3.3.1
qt6-kmssupport-private-devel: до 6.4.2-150500.3.3.1
qt6-sql-sqlite-debuginfo: до 6.4.2-150500.3.3.1
qt6-base-common-devel: до 6.4.2-150500.3.3.1
libQt6Concurrent6-debuginfo: до 6.4.2-150500.3.3.1
qt6-base-debuginfo: до 6.4.2-150500.3.3.1
libQt6Gui6-debuginfo: до 6.4.2-150500.3.3.1
libQt6DBus6: до 6.4.2-150500.3.3.1
libQt6Widgets6: до 6.4.2-150500.3.3.1
libQt6Network6: до 6.4.2-150500.3.3.1
libQt6Gui6: до 6.4.2-150500.3.3.1
qt6-network-tls-debuginfo: до 6.4.2-150500.3.3.1
libQt6OpenGL6: до 6.4.2-150500.3.3.1
libQt6Core6: до 6.4.2-150500.3.3.1
libQt6OpenGL6-debuginfo: до 6.4.2-150500.3.3.1
qt6-network-tls: до 6.4.2-150500.3.3.1
libQt6Core6-debuginfo: до 6.4.2-150500.3.3.1
qt6-base-debugsource: до 6.4.2-150500.3.3.1
libQt6Network6-debuginfo: до 6.4.2-150500.3.3.1
libQt6DBus6-debuginfo: до 6.4.2-150500.3.3.1
libQt6Widgets6-debuginfo: до 6.4.2-150500.3.3.1

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

Способ эксплуатации: Отправка 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: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: 2023-07-04 / 2023-07-04

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232780-1/

Краткое описание: Отказ в обслуживании в VMware Tanzu Application Service for VMs

Идентификатор уязвимости: CVE-2023-2650

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

Уязвимый продукт: VMware Tanzu Application Service for VMs: все версии
Isolation Segment: все версии
VMware Tanzu Operations Manager: до 2.10.59

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://tanzu.vmware.com/security/usn-6188-1

6

Краткое описание: Чтение локальных файлов в IBM CICS TX Advanced

Идентификатор уязвимости: CVE-2023-21930

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: IBM CICS TX Advanced: до 11.1.0.0 ifix11
IBM CICS TX Standard: до 11.1.0.0 ifix11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-05 / 2023-07-05

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7009485
- http://www.ibm.com/support/pages/node/7009483
- https://bdu.fstec.ru/vul/2023-02179

Краткое описание: Выполнение произвольного кода в FortiOS

Идентификатор уязвимости: CVE-2023-27997

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

Уязвимый продукт: FortiOS: 6.0.0 - 7.2.4
FortiProxy: 1.1.0 - 7.2.3
FortiOS-6K7K: 6.0.10 - 7.0.10

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

Способ эксплуатации: Отправка специально созданных запросов.

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: 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://fortiguard.fortinet.com/psirt/FG-IR-23-097
- http://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
- https://bdu.fstec.ru/vul/2023-03157

8

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-32393

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-03 / 2023-07-03

Ссылки на источник:

- http://support.apple.com/en-us/HT213606

9

Краткое описание: Выполнение произвольного кода в Artifex Ghostscript

Идентификатор уязвимости: CVE-2023-36664

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

Уязвимый продукт: Artifex Ghostscript: 9.00 - 10.01.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 8.4 AV:L/AC:L/PR:N/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: 2023-07-04 / 2023-07-04

Ссылки на источник:

- http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=0974e4f2ac0005d3731e0b5c13ebc7e965540f4d
- http://bugs.ghostscript.com/show_bug.cgi?id=706761
- http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=505eab7782b429017eb434b2b95120855f2b0e3c
- http://www.debian.org/security/2023/dsa-5446
- https://bdu.fstec.ru/vul/2023-03466