НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-05-22.1 | 22 мая 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-28756	cflinuxfs3	Сетевой	RLF	2023-05-22	✓
2	Высокая	CVE-2023-32159	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
3	Высокая	CVE-2023-32160	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
4	Высокая	CVE-2023-32161	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
5	Критическая	CVE-2022-4338	SUSE Linux Enterprise Server 12 SP2 BCL	Сетевой	ACE	2023-05-22	✓
6	Критическая	CVE-2022-4337	SUSE Linux Enterprise Server 12 SP2 BCL	Сетевой	DoS	2023-05-22	✓
7	Высокая	CVE-2022-32166	SUSE Linux Enterprise Server 12 SP2 BCL	Сетевой	DoS	2023-05-22	✓
8	Высокая	CVE-2023-32158	PDF-XChange Editor	Локальный	ACE	2023-05-22	✓
9	Высокая	CVE-2023-28755	cflinuxfs3	Сетевой	ACE	2023-05-22	✓
10	Высокая	CVE-2022-48303	tar (Ubuntu package)	Локальный	ACE	2023-05-22	✓
11	Высокая	CVE-2023-24805	Debian Linux	Сетевой	ACE	2023-05-22	✓
12	Высокая	CVE-2023-20189	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓

13	Высокая	CVE-2023-20162	Cisco Small Business 200 Series Smart Switches	Сетевой	OSI	2023-05-17	✓
14	Высокая	CVE-2023-20161	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
15	Высокая	CVE-2023-20160	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
16	Высокая	CVE-2023-20159	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
17	Высокая	CVE-2023-20158	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
18	Высокая	CVE-2023-20157	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
19	Высокая	CVE-2023-20156	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
20	Высокая	CVE-2023-20024	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓

1

Краткое описание: Чтение локальных файлов в cflinuxfs3

Идентификатор уязвимости: CVE-2023-28756

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: cflinuxfs3: 0.0.0 - 0.365.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 7.5 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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.366.0
- https://bdu.fstec.ru/vul/2023-02020

2

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32159

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-641/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

3

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32160

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-642/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

4

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32161

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-643/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

5

Краткое описание: Выполнение произвольного кода в SUSE Linux Enterprise Server 12 SP2 BCL

Идентификатор уязвимости: CVE-2022-4338

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: SUSE Linux Enterprise Server 12 SP2 BCL: 12-SP2
SUSE Linux Enterprise Server 12: SP2
SUSE Linux Enterprise High Performance Computing 12: SP2
openvswitch-dpdk-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-switch: до 2.5.11-25.34.1
openvswitch-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-debugsource: до 2.5.11-25.34.1
openvswitch: до 2.5.11-25.34.1
openvswitch-dpdk: до 2.5.11-25.34.1
openvswitch-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-debugsource: до 2.5.11-25.34.1
openvswitch-dpdk-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-switch: до 2.5.11-25.34.1

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232259-1/
- https://bdu.fstec.ru/vul/2023-00291

6

Краткое описание: Отказ в обслуживании в SUSE Linux Enterprise Server 12 SP2 BCL

Идентификатор уязвимости: CVE-2022-4337

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SUSE Linux Enterprise Server 12 SP2 BCL: 12-SP2
SUSE Linux Enterprise Server 12: SP2
SUSE Linux Enterprise High Performance Computing 12: SP2
openvswitch-dpdk-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-switch: до 2.5.11-25.34.1
openvswitch-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-debugsource: до 2.5.11-25.34.1
openvswitch: до 2.5.11-25.34.1
openvswitch-dpdk: до 2.5.11-25.34.1
openvswitch-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-debugsource: до 2.5.11-25.34.1
openvswitch-dpdk-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-switch: до 2.5.11-25.34.1

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: 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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232259-1/
- https://bdu.fstec.ru/vul/2023-00290

7

Краткое описание: Отказ в обслуживании в SUSE Linux Enterprise Server 12 SP2 BCL

Идентификатор уязвимости: CVE-2022-32166

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SUSE Linux Enterprise Server 12 SP2 BCL: 12-SP2
SUSE Linux Enterprise Server 12: SP2
SUSE Linux Enterprise High Performance Computing 12: SP2
openvswitch-dpdk-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-switch: до 2.5.11-25.34.1
openvswitch-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-debugsource: до 2.5.11-25.34.1
openvswitch: до 2.5.11-25.34.1
openvswitch-dpdk: до 2.5.11-25.34.1
openvswitch-debuginfo: до 2.5.11-25.34.1
openvswitch-dpdk-debugsource: до 2.5.11-25.34.1
openvswitch-dpdk-switch-debuginfo: до 2.5.11-25.34.1
openvswitch-switch: до 2.5.11-25.34.1

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: 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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.suse.com/support/update/announcement/2023/suse-su-20232259-1/

8

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2023-32158

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 9.5.368.0

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-640/
- http://www.tracker-software.com/product/pdf-xchange-editor/history

9

Краткое описание: Выполнение произвольного кода в cflinuxfs3

Идентификатор уязвимости: CVE-2023-28755

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: cflinuxfs3: 0.0.0 - 0.365.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.366.0

Краткое описание: Выполнение произвольного кода в tar (Ubuntu package)

Идентификатор уязвимости: CVE-2022-48303

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

Уязвимый продукт: tar (Ubuntu package): до 1.34+dfsg-1.2ubuntu0.1
23.04

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

10

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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-5900-2
- https://bdu.fstec.ru/vul/2023-00577

Краткое описание: Выполнение произвольного кода в Debian Linux

Идентификатор уязвимости: CVE-2023-24805

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

Уязвимый продукт: Debian Linux: все версии
cups-filters (Debian package): до 1.28.7-1+deb11u2

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

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2023-05-22 / 2023-05-22

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5407

Краткое описание: Выполнение произвольного кода в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20189

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27424
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32321

Краткое описание: Получение конфиденциальной информации в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20162

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

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

13

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32338
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27445

Краткое описание: Выполнение произвольного кода в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20161

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

14 **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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27444
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32334

Краткое описание: Выполнение произвольного кода в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20160

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

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

15

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27441
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32326

Краткое описание: Выполнение произвольного кода в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20159

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

16

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27425
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32323

17

Краткое описание: Отказ в обслуживании в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20158

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27403
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32318

Краткое описание: Отказ в обслуживании в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20157

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

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

18

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27394
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32315

Краткое описание: Отказ в обслуживании в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20156

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

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

19

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27393
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32313

Краткое описание: Отказ в обслуживании в Cisco Small Business 200 Series Smart Switches

Идентификатор уязвимости: CVE-2023-20024

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

Уязвимый продукт: Cisco Small Business 200 Series Smart Switches: все версии
Cisco Small Business 300 Series Managed Switches: все версии
Cisco Small Business 500 Series Stackable Managed Switches: все версии
Cisco 250 Series Smart Switches: до 2.5.9.16
Cisco 350 Series Managed Switches: до 2.5.9.16
Cisco 350X Series Stackable Managed Switches: до 2.5.9.16
Cisco 550X Series Stackable Managed Switches: до 2.5.9.16

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

20

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-17 / 2023-05-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe27386
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe32312