НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-05-15.1 | 15 мая 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-20046	Cisco StarOS	Сетевой	PE	2023-04-20	✓
2	Критическая	CVE-2023-29803	TOTOLINK X18	Сетевой	ACE	2023-04-19	✗
3	Критическая	CVE-2023-29798	TOTOLINK X18	Сетевой	ACE	2023-04-19	✗
4	Критическая	CVE-2023-29799	TOTOLINK X18	Сетевой	ACE	2023-04-19	✗
5	Критическая	CVE-2023-29800	TOTOLINK X18	Сетевой	ACE	2023-04-19	✗
6	Высокая	CVE-2022-41565	TIBCO EBX	Сетевой	XSS\CSS	2023-05-15	✓
7	Высокая	CVE-2023-0386	Debian Linux	Локальный	PE	2023-05-14	✓
8	Высокая	CVE-2022-41566	TIBCO EBX Add-ons	Сетевой	XSS\CSS	2023-05-15	✓
9	Критическая	CVE-2023-29268	TIBCO Spotfire Statistics Services	Сетевой	WLF	2023-05-15	✓
10	Критическая	CVE-2023-1834	Kinetix 5500	Сетевой	ACE	2023-05-12	✓
11	Высокая	CVE-2023-2133	Google ChromeOS LTS	Сетевой	ACE	2023-05-13	✓
12	Высокая	CVE-2023-2134	Google ChromeOS LTS	Сетевой	ACE	2023-05-13	✓
13	Высокая	CVE-2023-2135	Google ChromeOS LTS	Сетевой	ACE	2023-05-13	✓

Краткое описание: Повышение привилегий в Cisco StarOS

Идентификатор уязвимости: CVE-2023-20046

Идентификатор программной ошибки: CWE-255 Уязвимости, связанные с управлением учетными данными

Уязвимый продукт: Cisco StarOS: 21.22.0 - 21.28.m
Cisco ASR 5000 Series: все версии
Virtualized Packet Core - Distributed Instance (VPC-DI): все версии
Virtualized Packet Core - Single Instance (VPC-SI): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Повышение привилегий

1 **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: 2023-04-20 / 2023-04-20

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-ssh-privesc-BmWeJC3h
- https://bdu.fstec.ru/vul/2023-02354

2

Краткое описание: Выполнение произвольного кода в TOTOLINK X18

Идентификатор уязвимости: CVE-2023-29803

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLINK X18: 9.1.0cu.2024_B20220329

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2023-04-19 / 2023-04-19

Ссылки на источник:

- http://sore-pail-31b.notion.site/Command-Inject-1-4a37b0679f69478285d1ba640e5f0897

3

Краткое описание: Выполнение произвольного кода в TOTOLINK X18

Идентификатор уязвимости: CVE-2023-29798

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLINK X18: 9.1.0cu.2021_B20220326 - 9.1.0cu.2024_B20220329

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2023-04-19 / 2023-04-19

Ссылки на источник:

- http://sore-pail-31b.notion.site/Command-Injection-4-ea4969f635f54fe5b2f575e93443a4e0

4

Краткое описание: Выполнение произвольного кода в TOTOLINK X18

Идентификатор уязвимости: CVE-2023-29799

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLINK X18: 9.1.0cu.2021_B20220326 - 9.1.0cu.2024_B20220329

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2023-04-19 / 2023-04-19

Ссылки на источник:

- http://sore-pail-31b.notion.site/Command-Inject-6-3ee0faa243134ae2bc20e6670d80bada

5

Краткое описание: Выполнение произвольного кода в TOTOLINK X18

Идентификатор уязвимости: CVE-2023-29800

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLINK X18: 9.1.0cu.2021_B20220326 - 9.1.0cu.2024_B20220329

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2023-04-19 / 2023-04-19

Ссылки на источник:

- http://sore-pail-31b.notion.site/Command-Injection-5-e88b72309a3c4e20b7469b3679c0c7d9

Краткое описание: Межсайтовый скриптинг в TIBCO EBX

Идентификатор уязвимости: CVE-2022-41565

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: TIBCO EBX: 5.9.21 - 6.0.11
TIBCO Product and Service Catalog powered by TIBCO EBX: 1.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Межсайтовый скриптинг

6 **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: 8.7 AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-15 / 2023-05-15

Ссылки на источник:

- http://www.tibco.com/services/support/advisories

Краткое описание: Повышение привилегий в Debian Linux

Идентификатор уязвимости: CVE-2023-0386

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

Уязвимый продукт: Debian Linux: все версии
linux (Debian package): до 5.10.179-1

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

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

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: 7.8 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: 2023-05-14 / 2023-05-14

Ссылки на источник:

- http://www.debian.org/security/2023/dsa-5402
- https://bdu.fstec.ru/vul/2023-01572

8

Краткое описание: Межсайтовый скриптинг в TIBCO EBX Add-ons

Идентификатор уязвимости: CVE-2022-41566

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: TIBCO EBX Add-ons: 5.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Межсайтовый скриптинг

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-15 / 2023-05-15

Ссылки на источник:

- http://www.tibco.com/services/support/advisories

9

Краткое описание: Запись локальных файлов в TIBCO Spotfire Statistics Services

Идентификатор уязвимости: CVE-2023-29268

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: TIBCO Spotfire Statistics Services: 11.4.10 - 12.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись 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: 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: 2023-05-15 / 2023-05-15

Ссылки на источник:

- http://www.tibco.com/services/support/advisories

10

Краткое описание: Выполнение произвольного кода в Kinetix 5500

Идентификатор уязвимости: CVE-2023-1834

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Kinetix 5500: 7.13

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-05-12 / 2023-05-12

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139441
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-131-09

11

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2023-2133

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

Уязвимый продукт: Google ChromeOS LTS: до 108.0.5359.231

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

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

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: 2023-05-13 / 2023-05-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/05/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-02314

12

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2023-2134

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

Уязвимый продукт: Google ChromeOS LTS: до 108.0.5359.231

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

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

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: 2023-05-13 / 2023-05-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/05/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-02312

13

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2023-2135

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google ChromeOS LTS: до 108.0.5359.231

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

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

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:H/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: 2023-05-13 / 2023-05-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/05/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-02308