НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-06-07.1 | 7 июня 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-24540	Ubuntu	Сетевой	ACE	2023-06-06	✓
2	Критическая	CVE-2023-24538	Ubuntu	Сетевой	ACE	2023-06-06	✓
3	Высокая	CVE-2023-24537	Ubuntu	Сетевой	DoS	2023-06-06	✓
4	Высокая	CVE-2023-24534	Ubuntu	Сетевой	DoS	2023-06-06	✓
5	Высокая	CVE-2022-41724	Ubuntu	Сетевой	DoS	2023-06-06	✓
6	Критическая	CVE-2023-29961	D-Link DIR-605L version 1.17B01 BETA	Сетевой	ACE	2023-05-16	✗
7	Критическая	CVE-2023-31587	Tenda AC5 router V15.03.06.28	Сетевой	ACE	2023-05-16	✗
8	Высокая	CVE-2023-20189	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
9	Высокая	CVE-2023-20162	Cisco Small Business 200 Series Smart Switches	Сетевой	OSI	2023-05-17	✓
10	Высокая	CVE-2023-20161	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
11	Высокая	CVE-2023-20160	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓
12	Высокая	CVE-2023-20159	Cisco Small Business 200 Series Smart Switches	Сетевой	ACE	2023-05-17	✓

13	Высокая	CVE-2023-20158	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
14	Высокая	CVE-2023-20024	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
15	Высокая	CVE-2023-20156	Cisco Small Business 200 Series Smart Switches	Сетевой	DoS	2023-05-17	✓
16	Критическая	CVE-2023-33236	MXsecurity	Сетевой	ACE	2023-05-26	✓
17	Критическая	CVE-2023-33010	ATP series	Сетевой	ACE	2023-05-25	✓
18	Критическая	CVE-2023-33009	ATP series	Сетевой	ACE	2023-05-25	✓
19	Высокая	CVE-2023-33235	MXsecurity	Сетевой	ACE	2023-05-26	✓
20	Высокая	CVE-2023-25652	Red Hat OpenShift Container Platform	Сетевой	PE	2023-06-04	✓
21	Критическая	CVE-2023-23914	JBoss Core Services	Сетевой	OSI	2023-06-05	✓
22	Высокая	CVE-2022-43551	JBoss Core Services	Сетевой	OSI	2023-06-05	✓

1

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-24540

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

Уязвимый продукт: Ubuntu: 22.10 - 23.04
golang-1.20-src (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19 (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.20 (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.20-go (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19-src (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.19-go (Ubuntu package): до 1.19.8-1ubuntu0.1

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

Способ эксплуатации: Отправка специально созданных 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: 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://ubuntu.com/security/notices/USN-6140-1

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: 22.10 - 23.04
golang-1.20-src (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19 (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.20 (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.20-go (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19-src (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.19-go (Ubuntu package): до 1.19.8-1ubuntu0.1

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

Способ эксплуатации: Отправка специально сформированного запроса.

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

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6140-1

3

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2023-24537

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Ubuntu: 22.10 - 23.04
golang-1.20-src (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19 (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.20 (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.20-go (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19-src (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.19-go (Ubuntu package): до 1.19.8-1ubuntu0.1

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

Способ эксплуатации: Не определено

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

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6140-1

4

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2023-24534

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

Уязвимый продукт: Ubuntu: 22.10 - 23.04
golang-1.20-src (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19 (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.20 (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.20-go (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19-src (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.19-go (Ubuntu package): до 1.19.8-1ubuntu0.1

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

Способ эксплуатации: Не определено

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

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6140-1

5

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2022-41724

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

Уязвимый продукт: Ubuntu: 22.10 - 23.04
golang-1.20-src (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19 (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.20 (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.20-go (Ubuntu package): до 1.20.3-1ubuntu0.1
golang-1.19-src (Ubuntu package): до 1.19.8-1ubuntu0.1
golang-1.19-go (Ubuntu package): до 1.19.8-1ubuntu0.1

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

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6140-1

6

Краткое описание: Выполнение произвольного кода в D-Link DIR-605L version 1.17B01 BETA

Идентификатор уязвимости: CVE-2023-29961

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link DIR-605L version 1.17B01 BETA

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2023-05-16 / 2023-05-25

Ссылки на источник:

- https://github.com/Archerber/bug_submit/blob/main/D-Link/dir605l.md

Краткое описание: Выполнение произвольного кода в Tenda AC5 router V15.03.06.28

Идентификатор уязвимости: CVE-2023-31587

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Tenda AC5 router V15.03.06.28

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

7

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: 2023-05-16 / 2023-05-22

Ссылки на источник:

- https://github.com/yanbushuang/CVE/blob/main/TendaAC5.md
- https://www.tenda.com.cn/download/detail-2740.html
- https://www.tenda.com.cn/product/AC5.html

8

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.

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
- https://bdu.fstec.ru/vul/2023-02754

9

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: Отправка специально сформированных данных.

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
- https://bdu.fstec.ru/vul/2023-02758

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.

10

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

11

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.

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
- https://bdu.fstec.ru/vul/2023-02759

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.

Последствия эксплуатации: Выполнение произвольного кода

12

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
- https://bdu.fstec.ru/vul/2023-02662

13

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
- https://bdu.fstec.ru/vul/2023-02760

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.

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: 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
- https://bdu.fstec.ru/vul/2023-02733

15

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.

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
- https://bdu.fstec.ru/vul/2023-02734

Краткое описание: Выполнение произвольного кода в MXsecurity

Идентификатор уязвимости: CVE-2023-33236

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: MXsecurity: 1.0 - 1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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.

16

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: 2023-05-26 / 2023-05-26

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mxsecurity-command-injection-and-hardcoded-credential-vulnerabilities
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-145-01
- http://www.zerodayinitiative.com/advisories/ZDI-23-720/
- https://bdu.fstec.ru/vul/2023-01149

17

Краткое описание: Выполнение произвольного кода в ATP series

Идентификатор уязвимости: CVE-2023-33010

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

Уязвимый продукт: ATP series: 4.32 - 5.36 Patch 1
USG FLEX series: 4.50 - 5.36 Patch 1
USG FLEX 50W: 4.25 - 5.36 Patch 1
USG20W-VPN: 4.25 - 5.36 Patch 1
VPN series: 4.30 - 5.36 Patch 1
ZyWALL: 4.25 - 4.73 Patch 1
USG series: 4.25 - 4.73 Patch 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
- http://www.zyxel.com/global/en/support/security-advisories/zyxels-guidance-for-the-recent-attacks-on-the-zywall-devices
- https://bdu.fstec.ru/vul/2023-02796

18

Краткое описание: Выполнение произвольного кода в ATP series

Идентификатор уязвимости: CVE-2023-33009

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

Уязвимый продукт: ATP series: 4.32 - 5.36 Patch 1
USG FLEX series: 4.50 - 5.36 Patch 1
USG FLEX 50W: 4.25 - 5.36 Patch 1
USG20W-VPN: 4.25 - 5.36 Patch 1
VPN series: 4.30 - 5.36 Patch 1
ZyWALL: 4.25 - 4.73 Patch 1
USG series: 4.25 - 4.73 Patch 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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: 2023-05-25 / 2023-05-25

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
- http://www.zyxel.com/global/en/support/security-advisories/zyxels-guidance-for-the-recent-attacks-on-the-zywall-devices
- https://bdu.fstec.ru/vul/2023-02797

19

Краткое описание: Выполнение произвольного кода в MXsecurity

Идентификатор уязвимости: CVE-2023-33235

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

Уязвимый продукт: MXsecurity: 1.0 - 1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.2 AV:N/AC:L/PR:H/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: 2023-05-26 / 2023-05-26

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mxsecurity-command-injection-and-hardcoded-credential-vulnerabilities
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-145-01
- http://www.zerodayinitiative.com/advisories/ZDI-23-721/
- https://bdu.fstec.ru/vul/2023-01515

Краткое описание: Повышение привилегий в Red Hat OpenShift Container Platform

Идентификатор уязвимости: CVE-2023-25652

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

Уязвимый продукт: Red Hat OpenShift Container Platform: 4.13.0 - 4.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Повышение привилегий

20 **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: 2023-06-04 / 2023-06-04

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:3304

Краткое описание: Получение конфиденциальной информации в JBoss Core Services

Идентификатор уязвимости: CVE-2023-23914

Идентификатор программной ошибки: CWE-319 Передача важных данных в незашифрованном виде

Уязвимый продукт: JBoss Core Services: 2.4.37 SP8 - 2.4.51 SP1
jbcs-httpd24-openssl-pkcs11 (Red Hat package): до 0.4.10-33.el8jbcs
jbcs-httpd24-openssl-chil (Red Hat package): до 1.0.0-18.el8jbcs
jbcs-httpd24-mod_security (Red Hat package): до 2.9.3-24.el8jbcs
jbcs-httpd24-mod_proxy_cluster (Red Hat package): до 1.3.18-2.el8jbcs
jbcs-httpd24-mod_md (Red Hat package): до 2.4.0-20.el8jbcs
jbcs-httpd24-mod_http2 (Red Hat package): до 1.15.19-23.el8jbcs
jbcs-httpd24-httpd (Red Hat package): до 2.4.51-39.el8jbcs
jbcs-httpd24-curl (Red Hat package): до 8.0.1-1.el8jbcs
jbcs-httpd24-apr-util (Red Hat package): до 1.6.1-101.el8jbcs

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

21

Способ эксплуатации: Обход ограничений безопасности

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:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-05 / 2023-06-05

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:3354
- http://access.redhat.com/errata/RHSA-2023:3355
- https://bdu.fstec.ru/vul/2023-02154

Краткое описание: Получение конфиденциальной информации в JBoss Core Services

Идентификатор уязвимости: CVE-2022-43551

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: JBoss Core Services: 2.4.37 SP8 - 2.4.51 SP1
jbcs-httpd24-openssl-pkcs11 (Red Hat package): до 0.4.10-33.el8jbcs
jbcs-httpd24-openssl-chil (Red Hat package): до 1.0.0-18.el8jbcs
jbcs-httpd24-mod_security (Red Hat package): до 2.9.3-24.el8jbcs
jbcs-httpd24-mod_proxy_cluster (Red Hat package): до 1.3.18-2.el8jbcs
jbcs-httpd24-mod_md (Red Hat package): до 2.4.0-20.el8jbcs
jbcs-httpd24-mod_http2 (Red Hat package): до 1.15.19-23.el8jbcs
jbcs-httpd24-httpd (Red Hat package): до 2.4.51-39.el8jbcs
jbcs-httpd24-curl (Red Hat package): до 8.0.1-1.el8jbcs
jbcs-httpd24-apr-util (Red Hat package): до 1.6.1-101.el8jbcs

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

22 **Способ эксплуатации:** Открытие пользователем специально созданной вредоносной ссылки.

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: 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: 2023-06-05 / 2023-06-05

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:3354
- http://access.redhat.com/errata/RHSA-2023:3355
- https://bdu.fstec.ru/vul/2023-02157