НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-05-03.1 | 3 мая 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-29011	SonicWall GMS	Сетевой	SB	2024-05-01	✓
2	Высокая	CVE-2024-20378	Cisco IP Phone 6800, 7800 and 8800 Series with Multiplatform Firmware	Сетевой	OSI	2024-05-02	✓
3	Высокая	CVE-2024-20376	Cisco IP Phone 6800, 7800 and 8800 Series with Multiplatform Firmware	Сетевой	DoS	2024-05-02	✓
4	Высокая	CVE-2024-4058	Microsoft Edge	Сетевой	ACE	2024-04-29	✓
5	Высокая	CVE-2024-4060	Microsoft Edge	Сетевой	ACE	2024-04-29	✓
6	Критическая	CVE-2024-32038	Wazuh	Сетевой	ACE	2024-04-29	✓
7	Высокая	CVE-2024-4192	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-05-02	✓
8	Критическая	CVE-2023-5389	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	OSI	2024-04-26	✓
9	Высокая	CVE-2023-5392	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	OSI	2024-04-26	✓
10	Высокая	CVE-2023-5400	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓

11	Высокая	CVE-2023-5404	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓
12	Высокая	CVE-2023-5401	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓
13	Высокая	CVE-2023-5403	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓
14	Высокая	CVE-2023-5397	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓
15	Высокая	CVE-2023-5395	Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC	Сетевой	ACE	2024-04-26	✓
16	Высокая	CVE-2024-20281	Cisco Nexus Dashboard and Nexus Dashboard Hosted Services	Сетевой	XSS\CSS	2024-04-04	✓
17	Критическая	CVE-2024-3272	D-Link routers	Сетевой	ACE	2024-04-08	✗
18	Высокая	CVE-2024-3273	D-Link routers	Сетевой	ACE	2024-04-08	✗
19	Высокая	CVE-2023-41677	FortiOS and FortiProxy	Сетевой	OSI	2024-04-09	✓
20	Критическая	CVE-2023-45590	FortiClient for Linux	Сетевой	ACE	2024-04-09	✓

1

Краткое описание: Обход безопасности в SonicWall GMS

Идентификатор уязвимости: CVE-2024-29011

Идентификатор программной ошибки: CWE-259 Использование жестко закодированного пароля

Уязвимый продукт: SonicWall GMS: до 9.4.0 9.4-9400.1040

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Обход безопасности

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

Дата выявления / Дата обновления: 2024-05-01 / 2024-05-01

Ссылки на источник:

- http://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0007

2

Краткое описание: Получение конфиденциальной информации в Cisco IP Phone 6800, 7800 and 8800 Series with Multiplatform Firmware

Идентификатор уязвимости: CVE-2024-20378

Идентификатор программной ошибки: CWE-305 Обход аутентификации с помощью стороннего недостатка

Уязвимый продукт: IP Phone 6800 Series with Multiplatform Firmware: 12.0.4
IP Phone 7800 Series with Multiplatform Firmware: 12.0.4
Cisco IP Phone 8800 Series with Multiplatform Firmware: 12.0.4
Video Phone 8875 in Multiplatform Mode: 2.3.1.001

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Дата выявления / Дата обновления: 2024-05-02 / 2024-05-02

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-multi-vulns-cXAhCvS

Краткое описание: Отказ в обслуживании в Cisco IP Phone 6800, 7800 and 8800 Series with Multiplatform Firmware

Идентификатор уязвимости: CVE-2024-20376

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: IP Phone 6800 Series with Multiplatform Firmware: 12.0.4
IP Phone 7800 Series with Multiplatform Firmware: 12.0.4
Cisco IP Phone 8800 Series with Multiplatform Firmware: 12.0.4
Video Phone 8875 in Multiplatform Mode: 2.3.1.001

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

3 **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

Дата выявления / Дата обновления: 2024-05-02 / 2024-05-02

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-multi-vulns-cXAhCvS

4

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-4058

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 124.0.2478.67

Категория уязвимого продукта: Операционные системы Microsoft 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-29 / 2024-04-29

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-4058

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-4060

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 124.0.2478.67

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-29 / 2024-04-29

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-4060

6

Краткое описание: Выполнение произвольного кода в Wazuh

Идентификатор уязвимости: CVE-2024-32038

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

Уязвимый продукт: Wazuh: 3.8.0 - 4.7.1

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: 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

Дата выявления / Дата обновления: 2024-04-29 / 2024-04-29

Ссылки на источник:

- http://github.com/wazuh/wazuh/security/advisories/GHSA-fcpw-v3pg-c327
- http://www.zerodayinitiative.com/advisories/ZDI-24-397/

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-4192

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-G2: 2.0.0.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-02 / 2024-05-02

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-121-01

8

Краткое описание: Получение конфиденциальной информации в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5389

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04
- https://bdu.fstec.ru/vul/2024-00879

9

Краткое описание: Получение конфиденциальной информации в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5392

Идентификатор программной ошибки: CWE-1295 Избыточная информация в сообщениях отладки

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

10

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5400

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

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

11

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5404

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

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5401

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

12

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

13

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5403

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

14

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5397

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

15

Краткое описание: Выполнение произвольного кода в Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager and Safety Manager SC

Идентификатор уязвимости: CVE-2023-5395

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Safety Manager: R15x - R162.10
Safety Manager SC: R210.X - R212.1
Experion PKS: до R520.2 TCU4 HF2
Experion LX: до R520.2 TCU4 HF2
Experion PlantCruise: до R520.2 TCU4 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-26 / 2024-04-26

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-116-04

16

Краткое описание: Межсайтовый скриптинг в Cisco Nexus Dashboard and Nexus Dashboard Hosted Services

Идентификатор уязвимости: CVE-2024-20281

Идентификатор программной ошибки: CWE-352 Подделка межсайтового запроса (CSRF)

Уязвимый продукт: Nexus Dashboard: 2.3 - 3.1
Cisco Nexus Dashboard Fabric Controller (NDFC): 12.0 - 12.2.1
Cisco Nexus Dashboard Insights (NDI): 6.2 - 6.4
Cisco Nexus Dashboard Orchestrator (NDO): 4.1 - 4.3

Категория уязвимого продукта: Телекоммуникационное оборудование

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

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: 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

Дата выявления / Дата обновления: 2024-04-04 / 2024-04-04

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfccsrf-TEmZEfJ9

17

Краткое описание: Выполнение произвольного кода в D-Link routers

Идентификатор уязвимости: CVE-2024-3272

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

Уязвимый продукт: D-Link DNS-320L: все версии
D-Link DNS-325: все версии
D-Link DNS-327L: все версии
D-Link DNS-340L: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных 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

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://vuldb.com/?id.259283
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383
- https://bdu.fstec.ru/vul/2024-03256

Краткое описание: Выполнение произвольного кода в D-Link routers

Идентификатор уязвимости: CVE-2024-3273

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

Уязвимый продукт: D-Link DNS-320L: все версии
D-Link DNS-325: все версии
D-Link DNS-327L: все версии
D-Link DNS-340L: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

18 **Последствия эксплуатации:** Выполнение произвольного кода

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

Оценка CVSSv3: 7.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://vuldb.com/?id.259284
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383
- https://bdu.fstec.ru/vul/2024-02740

Краткое описание: Получение конфиденциальной информации в FortiOS and FortiProxy

Идентификатор уязвимости: CVE-2023-41677

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: FortiOS: 6.0.0 - 7.4.1
FortiProxy: 1.0.0 - 7.4.1

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

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

Последствия эксплуатации: Получение конфиденциальной информации

19 **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

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-493
- https://bdu.fstec.ru/vul/2024-03235

Краткое описание: Выполнение произвольного кода в FortiClient for Linux

Идентификатор уязвимости: CVE-2023-45590

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

Уязвимый продукт: FortiClient (Linux): 7.0.0 - 7.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-087