НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-08.1 | 8 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-40464	Sierra Wireless AirLink with ALEOS firmware	Сетевой	OSI	2023-12-08	✓
2	Высокая	CVE-2023-40463	Sierra Wireless AirLink with ALEOS firmware	Сетевой	LoI	2023-12-08	✓
3	Высокая	CVE-2023-40462	Sierra Wireless AirLink with ALEOS firmware	Сетевой	DoS	2023-12-08	✓
4	Высокая	CVE-2023-40461	Sierra Wireless AirLink with ALEOS firmware	Сетевой	XSS\CSS	2023-12-08	✓
5	Высокая	CVE-2023-40459	Sierra Wireless AirLink with ALEOS firmware	Сетевой	DoS	2023-12-08	✓
6	Высокая	CVE-2023-40458	Sierra Wireless AirLink with ALEOS firmware	Сетевой	DoS	2023-12-08	✓
7	Критическая	CVE-2023-22524	Atlassian Companion App for MacOS	Сетевой	ACE	2023-12-06	✓
8	Критическая	CVE-2023-22523	Atlassian Assets Discovery	Сетевой	OSI	2023-12-06	✓
9	Высокая	CVE-2023-5247	Mitsubishi Electric FA Engineering Software Products	Локальный	ACE	2023-12-05	✗
10	Высокая	CVE-2023-0464	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
11	Критическая	CVE-2023-38408	Dell EMC Enterprise SONiC	Сетевой	ACE	2023-12-01	✓

12	Высокая	CVE-2022-46285	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
13	Высокая	CVE-2022-44617	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
14	Высокая	CVE-2022-4883	Dell EMC Enterprise SONiC	Сетевой	PE	2023-12-01	✓
15	Высокая	CVE-2023-32067	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
16	Высокая	CVE-2023-3138	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
17	Высокая	CVE-2022-48560	Dell EMC Enterprise SONiC	Сетевой	DoS	2023-12-01	✓
18	Высокая	CVE-2023-2610	Dell EMC Enterprise SONiC	Локальный	ACE	2023-12-01	✓
19	Высокая	CVE-2023-24329	Dell EMC Enterprise SONiC	Сетевой	SB	2023-12-01	✓
20	Критическая	CVE-2022-48565	Dell EMC Enterprise SONiC	Сетевой	RLF	2023-12-01	✓
21	Высокая	CVE-2023-5944	Delta Industrial Automation DOPSoft	Локальный	ACE	2023-12-01	✗
22	Высокая	CVE-2023-5909	Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator	Сетевой	OSI	2023-12-04	✓
23	Критическая	CVE-2023-5908	Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator	Сетевой	DoS	2023-12-04	✓
24	Высокая	CVE-2023-48963	Tenda i6	Сетевой	DoS	2023-11-30	✓

25	Высокая	CVE-2023-48964	Tenda i6	Сетевой	DoS	2023-11-30	✓
26	Критическая	CVE-2023-45483	Tenda AC10	Сетевой	DoS	2023-11-29	✓
27	Критическая	CVE-2023-45482	Tenda AC10	Сетевой	DoS	2023-11-29	✓
28	Критическая	CVE-2023-45481	Tenda AC10	Сетевой	DoS	2023-11-29	✓
29	Критическая	CVE-2023-45480	Tenda AC10	Сетевой	DoS	2023-11-29	✓

1

Краткое описание: Получение конфиденциальной информации в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40464

Идентификатор программной ошибки: CWE-321 Использование жестко закодированного ключа шифрования

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/#sthash.oFyaRKPf.dpbs

2

Краткое описание: Потеря целостности в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40463

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

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: потеря целостности

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: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/#sthash.oFyaRKPf.dpbs

3

Краткое описание: Отказ в обслуживании в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40462

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

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Дата выявления / Дата обновления: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/#sthash.oFyaRKPf.dpbs

4

Краткое описание: Межсайтовый скриптинг в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40461

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/#sthash.oFyaRKPf.dpbs

5

Краткое описание: Отказ в обслуживании в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40459

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

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: 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: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/#sthash.oFyaRKPf.dpbs

6

Краткое описание: Отказ в обслуживании в Sierra Wireless AirLink with ALEOS firmware

Идентификатор уязвимости: CVE-2023-40458

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

Уязвимый продукт: Sierra Wireless AirLink with ALEOS firmware: до 4.17.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Дата выявления / Дата обновления: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-341-06
- http://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2023-006/

7

Краткое описание: Выполнение произвольного кода в Atlassian Companion App for MacOS

Идентификатор уязвимости: CVE-2023-22524

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Atlassian Companion App for MacOS: до 2.0.0

Категория уязвимого продукта: Средства защиты информации

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: 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: 2023-12-06 / 2023-12-06

Ссылки на источник:

- http://jira.atlassian.com/browse/CONFSERVER-93453
- http://confluence.atlassian.com/security/cve-2023-22524-rce-vulnerability-in-atlassian-companion-app-for-macos-1319249492.html

8

Краткое описание: Получение конфиденциальной информации в Atlassian Assets Discovery

Идентификатор уязвимости: CVE-2023-22523

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Atlassian Assets Discovery: до 6.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 9.8 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: 2023-12-06 / 2023-12-06

Ссылки на источник:

- http://jira.atlassian.com/browse/JSDSERVER-14893
- http://support.atlassian.com/jira-service-management-cloud/docs/install-asset-discovery-agents/
- http://support.atlassian.com/jira-service-management-cloud/docs/what-are-asset-discovery-agents/
- http://confluence.atlassian.com/security/cve-2023-22523-remote-code-execution-vulnerability-in-assets-discovery-1319248914.html
- http://confluence.atlassian.com/security/cve-2023-22523-rce-vulnerability-in-assets-discovery-1319248914.html

Краткое описание: Выполнение произвольного кода в Mitsubishi Electric FA Engineering Software Products

Идентификатор уязвимости: CVE-2023-5247

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: Mitsubishi Electric FA Engineering Software Products:
GX Works3: все версии
MELSOFT iQ AppPortal: все версии
MELSOFT Navigator: все версии
Motion Control Setting: все версии
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

9

Последствия эксплуатации: выполнение произвольного кода

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

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: 2023-12-05 / 2023-12-05

Ссылки на источник:

- http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-016_en.pdf
- http://jvn.jp/vu/JVNVU93383160/
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-334-04

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-0464

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

10 **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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-02108

11

Краткое описание: Выполнение произвольного кода в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-38408

Идентификатор программной ошибки: CWE-428 Отсутствие кавычек вокруг элемента в пути поиска

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-03950

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2022-46285

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

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-00390

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2022-44617

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

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: отказ в обслуживании

13 **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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-00389

Краткое описание: Повышение привилегий в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2022-4883

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-00388

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-32067

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

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

15 **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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-07649

16

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-3138

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

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

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-03596

Краткое описание: Отказ в обслуживании в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2022-48560

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

17 **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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities

18

Краткое описание: Выполнение произвольного кода в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-2610

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Dell EMC Enterprise SONiC: до 4.1.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-03861

Краткое описание: Обход безопасности в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2023-24329

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправки специально сформированного запроса.

Последствия эксплуатации: обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-04978

Краткое описание: Чтение локальных файлов в Dell EMC Enterprise SONiC

Идентификатор уязвимости: CVE-2022-48565

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Dell EMC Enterprise SONiC:
Enterprise SONiC: до 4.1.2
Fixed software versions

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: чтение локальных файлов

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: 9.8 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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000219487/dsa-2023-402-security-update-for-dell-emc-enterprise-sonic-distribution-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06655

Краткое описание: Выполнение произвольного кода в Delta Industrial Automation DOPSoft

Идентификатор уязвимости: CVE-2023-5944

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Delta Industrial Automation DOPSoft: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

21

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

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: 2023-12-01 / 2023-12-01

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-334-01

Краткое описание: Получение конфиденциальной информации в Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator

Идентификатор уязвимости: CVE-2023-5909

Идентификатор программной ошибки: CWE-297 Некорректная проверка сертификатов с несоответствием узла

Уязвимый продукт: Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator:
Kepware KepServerEX: 6.14.263.0
ThingWorx Kepware Server: 6.14.263.0
ThingWorx Industrial Connectivity: все версии
ThingWorx Kepware Edge: 1.7
OPC Aggregator: 6.14
Industrial Gateway Server: 7.614

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

22

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: 2023-12-04 / 2023-12-04

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-334-03
- http://www.ptc.com/en/support/article/CS405439

Краткое описание: Отказ в обслуживании в Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator

Идентификатор уязвимости: CVE-2023-5908

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

Уязвимый продукт: Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server, PTC KEPServerEX, ThingWorx and OPC-Aggregator:
Kepware KepServerEX: 6.14.263.0
ThingWorx Kepware Server: 6.14.263.0
ThingWorx Industrial Connectivity: все версии
ThingWorx Kepware Edge: 1.7
OPC Aggregator: 6.14
Industrial Gateway Server: 7.614

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

23

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-04 / 2023-12-04

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-334-03
- http://www.ptc.com/en/support/article/CS405439

Краткое описание: Отказ в обслуживании в Tenda i6

Идентификатор уязвимости: CVE-2023-48963

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i6: версии 1.0.0.8(3856)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

24

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: 2023-11-30 / 2023-11-30

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda i6

Идентификатор уязвимости: CVE-2023-48964

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda i6: версии 1.0.0.8(3856)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

25

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: 2023-11-30 / 2023-11-30

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda AC10

Идентификатор уязвимости: CVE-2023-45483

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC10: версии 16.03.10.13_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

26

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: 2023-11-29 / 2023-11-29

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda AC10

Идентификатор уязвимости: CVE-2023-45482

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC10: версии 16.03.10.13_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

27

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: 2023-11-29 / 2023-11-29

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda AC10

Идентификатор уязвимости: CVE-2023-45481

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC10: версии 16.03.10.13_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

28

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: 2023-11-29 / 2023-11-29

Ссылки на источник:

Краткое описание: Отказ в обслуживании в Tenda AC10

Идентификатор уязвимости: CVE-2023-45480

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC10: версии 16.03.10.13_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

29

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: 2023-11-29 / 2023-11-29

Ссылки на источник: