НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-06-19.1 | 19 июня 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-32460	Dell PowerFlex Appliance	Локальный	PE	2024-06-14	✓
2	Высокая	CVE-2023-23583	Dell PowerFlex Appliance	Локальный	ACE	2024-06-14	✓
3	Высокая	CVE-2024-20267	Dell PowerFlex Appliance	Сетевой	DoS	2024-06-14	✓
4	Высокая	CVE-2024-37369	Rockwell Automation FactoryTalk View SE	Локальный	PE	2024-06-14	✓
5	Высокая	CVE-2024-37367	Rockwell Automation FactoryTalk View SE	Сетевой	SB	2024-06-14	✓
6	Высокая	CVE-2024-37368	Rockwell Automation FactoryTalk View SE	Сетевой	SB	2024-06-14	✓
7	Высокая	CVE-2024-26275	Siemens Teamcenter Visualization and JT2Go	Локальный	OSI	2024-06-14	✓
8	Высокая	CVE-2024-37029	Fuji Electric Tellus Lite V-Simulator	Локальный	ACE	2024-06-14	✓
9	Высокая	CVE-2024-37022	Fuji Electric Tellus Lite V-Simulator	Локальный	ACE	2024-06-14	✓
10	Высокая	CVE-2024-5700	Mozilla Thunderbird	Сетевой	ACE	2024-06-14	✓
11	Высокая	CVE-2024-5696	Mozilla Thunderbird	Сетевой	ACE	2024-06-14	✓
12	Высокая	CVE-2024-5688	Mozilla Thunderbird	Сетевой	ACE	2024-06-14	✓

13	Высокая	CVE-2024-5702	Mozilla Thunderbird	Сетевой	ACE	2024-06-14	✓
14	Высокая	CVE-2024-33871	Artifex Ghostscript	Сетевой	ACE	2024-06-13	✓
15	Высокая	CVE-2024-5830	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
16	Высокая	CVE-2024-5835	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
17	Высокая	CVE-2024-5844	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
18	Высокая	CVE-2024-5833	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
19	Высокая	CVE-2024-5834	Microsoft Edge	Сетевой	OSI	2024-06-13	✓
20	Высокая	CVE-2024-5837	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
21	Высокая	CVE-2024-5832	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
22	Высокая	CVE-2024-5831	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
23	Высокая	CVE-2024-5836	Microsoft Edge	Сетевой	OSI	2024-06-13	✓
24	Высокая	CVE-2024-5839	Microsoft Edge	Сетевой	OSI	2024-06-13	✓
25	Высокая	CVE-2024-5838	Microsoft Edge	Сетевой	ACE	2024-06-13	✓
26	Высокая	CVE-2024-5843	Microsoft Edge	Сетевой	OSI	2024-06-13	✓
27	Критическая	CVE-2023-38545	Dell NetWorker Server	Сетевой	ACE	2024-06-13	✓

28	Критическая	CVE-2024-30300	Adobe FrameMaker Publishing Server	Сетевой	OSI	2024-06-13	✓
29	Критическая	CVE-2024-30299	Adobe FrameMaker Publishing Server	Сетевой	SB	2024-06-13	✓
30	Высокая	CVE-2023-3341	Dell SmartFabric OS10	Сетевой	DoS	2024-06-13	✓
31	Высокая	CVE-2024-0985	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	PE	2024-06-13	✓
32	Высокая	CVE-2023-6516	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
33	Высокая	CVE-2023-5679	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
34	Высокая	CVE-2023-5517	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
35	Высокая	CVE-2023-50387	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓
36	Высокая	CVE-2023-4408	Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software	Сетевой	DoS	2024-06-13	✓

1

Краткое описание: Повышение привилегий в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2023-32460

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: PowerFlex Appliance: до IC 45.374.00

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000223699/dsa-2024-161-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities

2

Краткое описание: Выполнение произвольного кода в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2023-23583

Идентификатор программной ошибки: CWE-1281 Последовательность инструкций процессора приводит к непредусмотренному поведению (Halt and Catch Fire)

Уязвимый продукт: PowerFlex Appliance: до IC 45.374.00

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000223699/dsa-2024-161-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-07325

3

Краткое описание: Отказ в обслуживании в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2024-20267

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

Уязвимый продукт: PowerFlex Appliance: до IC 45.374.00

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000223699/dsa-2024-161-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01750

4

Краткое описание: Повышение привилегий в Rockwell Automation FactoryTalk View SE

Идентификатор уязвимости: CVE-2024-37369

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: FactoryTalk View SE: 12.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-165-17
- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1674.html

5

Краткое описание: Обход безопасности в Rockwell Automation FactoryTalk View SE

Идентификатор уязвимости: CVE-2024-37367

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FactoryTalk View SE: 12.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных 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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-165-16
- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1675.html

6

Краткое описание: Обход безопасности в Rockwell Automation FactoryTalk View SE

Идентификатор уязвимости: CVE-2024-37368

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FactoryTalk View SE: 11.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-165-18
- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1676.html

Краткое описание: Получение конфиденциальной информации в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2024-26275

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Teamcenter Visualization: 14.2 - 2312
JT2Go: до 2312.0004

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-771940.txt
- https://bdu.fstec.ru/vul/2024-03168

8

Краткое описание: Выполнение произвольного кода в Fuji Electric Tellus Lite V-Simulator

Идентификатор уязвимости: CVE-2024-37029

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tellus Lite V-Simulator: до 4.0.20.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-165-14
- http://www.zerodayinitiative.com/advisories/ZDI-24-681/
- http://www.zerodayinitiative.com/advisories/ZDI-24-680/
- http://www.zerodayinitiative.com/advisories/ZDI-24-679/

9

Краткое описание: Выполнение произвольного кода в Fuji Electric Tellus Lite V-Simulator

Идентификатор уязвимости: CVE-2024-37022

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tellus Lite V-Simulator: до 4.0.20.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-165-14
- http://www.zerodayinitiative.com/advisories/ZDI-24-678/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-5700

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.11.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-28/

11

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-5696

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

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.11.1

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: 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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-28/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-5688

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.11.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 8.8 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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-28/

13

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-5702

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 115.11.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-06-14 / 2024-06-14

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-28/

14

Краткое описание: Выполнение произвольного кода в Artifex Ghostscript

Идентификатор уязвимости: CVE-2024-33871

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Ghostscript: 9.00 - 10.03.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://bugzilla.redhat.com/show_bug.cgi?id=2283508
- http://bugs.ghostscript.com/show_bug.cgi?id=707754
- http://ghostscript.readthedocs.io/en/gs10.03.1/News.html
- http://cgit.ghostscript.com/cgi-bin/cgit.cgi/ghostpdl.git/commit/?id=7145885041bb52cc23964f0aa2aec1b1c82b5908

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5830

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5830

16

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5835

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5835

17

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5844

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.5 AV:N/AC:H/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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5844

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5833

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

18 **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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5833

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5834

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5834

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5837

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5837

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5832

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

21 **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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5832

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5831

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

22 **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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5831

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5836

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

23 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5836

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5839

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5839

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5838

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5838

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5843

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.92

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5843

27

Краткое описание: Выполнение произвольного кода в Dell NetWorker Server

Идентификатор уязвимости: CVE-2023-38545

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

Уязвимый продукт: EMC NetWorker Server: до 19.10.0.2

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000223914/dsa-2024-166-security-update-for-dell-networker-curl-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06576

Краткое описание: Получение конфиденциальной информации в Adobe FrameMaker Publishing Server

Идентификатор уязвимости: CVE-2024-30300

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

Уязвимый продукт: Adobe FrameMaker Publishing Server: 2020 Update 3 - 2022.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html

Краткое описание: Обход безопасности в Adobe FrameMaker Publishing Server

Идентификатор уязвимости: CVE-2024-30299

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe FrameMaker Publishing Server: 2020 Update 3 - 2022.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html

30

Краткое описание: Отказ в обслуживании в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2023-3341

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

Уязвимый продукт: SmartFabric OS10: 10.5.5.8

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities
- https://bdu.fstec.ru/vul/2023-06079

31

Краткое описание: Повышение привилегий в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2024-0985

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01121

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-6516

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

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

32 **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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities

33

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-5679

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-04269

34

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-5517

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-02902

35

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-50387

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

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01359

36

Краткое описание: Отказ в обслуживании в Dell APEX Cloud Platform for Microsoft Azure and Dell APEX Cloud Platform Foundation Software

Идентификатор уязвимости: CVE-2023-4408

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

Уязвимый продукт: Azure Stack: до 10.2402

Категория уязвимого продукта: Операционные системы Microsoft 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

Дата выявления / Дата обновления: 2024-06-13 / 2024-06-13

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000224464/dsa-2024-129-security-update-for-dell-apex-cloud-platform-for-microsoft-azure-and-dell-apex-cloud-platform-foundation-software-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-02883