НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-10.1 | 10 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-51438	Siemens SIMATIC IPCs	Сетевой	SB	2024-01-10	✗
2	Высокая	CVE-2023-51746	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2024-01-10	✓
3	Высокая	CVE-2023-51745	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2024-01-10	✓
4	Высокая	CVE-2023-51439	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2024-01-10	✓
5	Критическая	CVE-2023-49621	Siemens SIMATIC CN 4100	Сетевой	SB	2024-01-10	✓
6	Высокая	CVE-2023-49252	Siemens SIMATIC CN 4100	Сетевой	DoS	2024-01-10	✓
7	Высокая	CVE-2023-49251	Siemens SIMATIC CN 4100	Сетевой	SB	2024-01-10	✓
8	Критическая	CVE-2024-0057	Microsoft NET, .NET Framework, and Visual Studio	Сетевой	SB	2024-01-10	✓
9	Высокая	CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider	Сетевой	SB	2024-01-10	✓
10	Высокая	CVE-2024-20713	Adobe Substance 3D Stager	Сетевой	ACE	2024-01-09	✓
11	Высокая	CVE-2024-0333	Google Chrome	Сетевой	ACE	2024-01-09	✓
12	Высокая	CVE-2024-20677	Microsoft Office	Локальный	ACE	2024-01-09	✓

13	Высокая	CVE-2024-21325	Microsoft Printer Metadata Troubleshooter Tool	Локальный	ACE	2024-01-09	✓
14	Высокая	CVE-2023-36639	Fortinet FortiProxy	Сетевой	ACE	2023-12-14	✓
15	Высокая	CVE-2023-48782	Fortinet FortiWLM	Сетевой	ACE	2023-12-12	✓
16	Критическая	CVE-2023-49004	D-Link DIR-850L	Сетевой	DoS	2023-12-19	✓
17	Критическая	CVE-2023-48842	D-Link Go-RT-AT750	Сетевой	DoS	2023-12-01	✓
18	Критическая	CVE-2023-6581	D-Link DAR-7000	Сетевой	SB	2023-12-07	✓
19	Высокая	CVE-2023-44252	Fortinet FortiWAN	Сетевой	PE	2023-11-20	✓
20	Высокая	CVE-2023-44251	Fortinet FortiWAN	Сетевой	ACE	2023-11-20	✓
21	Высокая	CVE-2023-4232	oFono	Сетевой	ACE	2024-01-03	✓
22	Высокая	CVE-2023-4233	oFono	Сетевой	ACE	2024-01-03	✓
23	Высокая	CVE-2023-4234	oFono	Сетевой	ACE	2024-01-03	✓
24	Высокая	CVE-2023-2794	oFono	Сетевой	ACE	2024-01-03	✓
25	Высокая	CVE-2023-39191	Google ChromeOS	Локальный	PE	2024-01-09	✓
26	Высокая	CVE-2023-6509	Google ChromeOS	Сетевой	ACE	2024-01-09	✓
27	Высокая	CVE-2023-6508	Google ChromeOS	Сетевой	ACE	2024-01-09	✓

28	Высокая	CVE-2023-7024	Google ChromeOS	Сетевой	ACE	2024-01-09	✓
29	Критическая	CVE-2023-51714	Qt	Сетевой	ACE	2024-01-08	✓
30	Критическая	CVE-2022-43634	QNAP operating system	Сетевой	ACE	2024-01-08	✓
31	Высокая	CVE-2024-0225	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-01-04	✓
32	Высокая	CVE-2024-0224	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-01-04	✓
33	Высокая	CVE-2023-44487	HPE Unified OSS Console Assurance Monitoring (UOCAM)	Сетевой	DoS	2024-01-04	✓
34	Высокая	CVE-2024-0223	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-01-04	✓
35	Высокая	CVE-2024-0222	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-01-04	✓
36	Высокая	CVE-2022-32231	Dell PowerScale OneFS	Локальный	ACE	2024-01-05	✓
37	Высокая	CVE-2022-4450	Dell PowerScale OneFS	Сетевой	DoS	2024-01-05	✓
38	Высокая	CVE-2023-0215	Dell PowerScale OneFS	Сетевой	DoS	2024-01-05	✓
39	Высокая	CVE-2023-49964	Hyland Alfresco Community Edition	Сетевой	ACE	2024-01-05	✗
40	Высокая	CVE-2023-44452	Linux Mint Xreader	Локальный	ACE	2024-01-04	✓
41	Высокая	CVE-2021-3712	Dell PowerScale OneFS	Сетевой	OSI	2024-01-05	✓
42	Критическая	CVE-2021-3711	Dell PowerScale OneFS	Сетевой	ACE	2024-01-05	✓

43	Высокая	CVE-2023-44451	Linux Mint Xreader	Локальный	RLF	2024-01-04	✓
44	Высокая	CVE-2022-0778	Dell PowerScale OneFS	Сетевой	DoS	2024-01-05	✓

1

Краткое описание: Обход безопасности в Siemens SIMATIC IPCs

Идентификатор уязвимости: CVE-2023-51438

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SIMATIC IPC1047E: все версии
SIMATIC IPC847E: все версии
SIMATIC IPC647E: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-702935.txt

2

Краткое описание: Выполнение произвольного кода в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2023-51746

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Teamcenter Visualization: 13.3 - 14.3
JT2Go: до 14.3.0.6

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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf

3

Краткое описание: Выполнение произвольного кода в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2023-51745

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Teamcenter Visualization: 13.3 - 14.3
JT2Go: до 14.3.0.6

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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf

4

Краткое описание: Выполнение произвольного кода в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2023-51439

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Teamcenter Visualization: 13.3 - 14.3
JT2Go: до 14.3.0.6

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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf

5

Краткое описание: Обход безопасности в Siemens SIMATIC CN 4100

Идентификатор уязвимости: CVE-2023-49621

Идентификатор программной ошибки: Не определено

Уязвимый продукт: SIMATIC CN 4100: до 2.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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: 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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf

6

Краткое описание: Отказ в обслуживании в Siemens SIMATIC CN 4100

Идентификатор уязвимости: CVE-2023-49252

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SIMATIC CN 4100: до 2.7

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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf

7

Краткое описание: Обход безопасности в Siemens SIMATIC CN 4100

Идентификатор уязвимости: CVE-2023-49251

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: SIMATIC CN 4100: до 2.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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: 8.8 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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf

8

Краткое описание: Обход безопасности в Microsoft NET, .NET Framework, and Visual Studio

Идентификатор уязвимости: CVE-2024-0057

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Visual Studio: 2022 version 17.2 - 2022 version 17.8
Microsoft .NET Framework: 2.0 Service Pack 2 - 4.8.1
.NET: 6.0.0 - 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057

9

Краткое описание: Обход безопасности в Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider

Идентификатор уязвимости: CVE-2024-0056

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: System.Data.SqlClient: все версии
Microsoft.Data.SqlClient: 2.1 - 5.1
Visual Studio: 2022 version 17.2 - 2022 version 17.8
Microsoft SQL Server: 2022
Microsoft .NET Framework: 2.0 Service Pack 2 - 4.8.1
.NET: 6.0.0 - 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2024-20713

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Substance 3D Stager: 2.0.0 - 2.1.3

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: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0333

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 120.0.6099.62 - 120.0.6099.200

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

11 **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: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_9.html

12

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2024-20677

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office: 2016 - 2019
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 7.8 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: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-20677

13

Краткое описание: Выполнение произвольного кода в Microsoft Printer Metadata Troubleshooter Tool

Идентификатор уязвимости: CVE-2024-21325

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Printer Metadata Troubleshooter Tool: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 7.8 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: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21325

14

Краткое описание: Выполнение произвольного кода в Fortinet FortiProxy

Идентификатор уязвимости: CVE-2023-36639

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: Fortinet FortiProxy: до версии 7.2.

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

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-14 / 2023-12-14

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-138
- https://bdu.fstec.ru/vul/2023-08764

Краткое описание: Выполнение произвольного кода в Fortinet FortiWLM

Идентификатор уязвимости: CVE-2023-48782

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

Уязвимый продукт: Fortinet FortiWLM: до версии 8.6.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-08752

16

Краткое описание: Отказ в обслуживании в D-Link DIR-850L

Идентификатор уязвимости: CVE-2023-49004

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

Уязвимый продукт: D-Link DIR-850L: версии.B1_FW223WWb01.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

Оценка CVSSv3: 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: 2023-12-19 / 2023-12-22

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-08998

Краткое описание: Отказ в обслуживании в D-Link Go-RT-AT750

Идентификатор уязвимости: CVE-2023-48842

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

Уязвимый продукт: D-Link Go-RT-AT750: до версии 101b03.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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: 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 / 2023-12-06

Ссылки на источник:

- https://bdu.fstec.ru/vul/2023-08699

Краткое описание: Обход безопасности в D-Link DAR-7000

Идентификатор уязвимости: CVE-2023-6581

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: D-Link DAR-7000: до версии 2.3.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: обход безопасности

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: 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: 2023-12-07 / 2023-12-07

Ссылки на источник:

- https://github.com/flyyue2001/cve/blob/main/D-LINK%20-DAR-7000_sql_workidajax.md

19

Краткое описание: Повышение привилегий в Fortinet FortiWAN

Идентификатор уязвимости: CVE-2023-44252

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Fortinet FortiWAN: до версии 5.2.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

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: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: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-061
- https://bdu.fstec.ru/vul/2023-08823

20

Краткое описание: Выполнение произвольного кода в Fortinet FortiWAN

Идентификатор уязвимости: CVE-2023-44251

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Fortinet FortiWAN: до версии 5.2.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-20 / 2023-11-20

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-265
- https://bdu.fstec.ru/vul/2023-08822

Краткое описание: Выполнение произвольного кода в oFono

Идентификатор уязвимости: CVE-2023-4232

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: oFono: 2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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: 8.1 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: 2024-01-03 / 2024-01-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1860/

Краткое описание: Выполнение произвольного кода в oFono

Идентификатор уязвимости: CVE-2023-4233

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: oFono: 2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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: 8.1 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: 2024-01-03 / 2024-01-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1859/
- https://bdu.fstec.ru/vul/2023-09050

23

Краткое описание: Выполнение произвольного кода в oFono

Идентификатор уязвимости: CVE-2023-4234

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: oFono: 2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-01-03 / 2024-01-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1858/
- https://bdu.fstec.ru/vul/2023-09111

Краткое описание: Выполнение произвольного кода в oFono

Идентификатор уязвимости: CVE-2023-2794

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: oFono: 2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-03 / 2024-01-03

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1861/

Краткое описание: Повышение привилегий в Google ChromeOS

Идентификатор уязвимости: CVE-2023-39191

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Chrome OS: до 120.0.6099.203

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

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2023-06203

26

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2023-6509

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 120.0.6099.203

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

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

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2023-08557

27

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2023-6508

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 120.0.6099.203

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

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

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2023-09063

28

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2023-7024

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

Уязвимый продукт: Chrome OS: до 120.0.6099.203

Категория уязвимого продукта: Unix-подобные операционные системы 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-chromeos.html
- https://bdu.fstec.ru/vul/2023-09068

29

Краткое описание: Выполнение произвольного кода в Qt

Идентификатор уязвимости: CVE-2023-51714

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

Уязвимый продукт: Qt: 5.15 - 6.6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-01-08 / 2024-01-08

Ссылки на источник:

- http://codereview.qt-project.org/c/qt/qtbase/+/524864
- http://codereview.qt-project.org/c/qt/qtbase/+/524865/3
- https://bdu.fstec.ru/vul/2024-00093

Краткое описание: Выполнение произвольного кода в QNAP operating system

Идентификатор уязвимости: CVE-2022-43634

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

Уязвимый продукт: QuTS hero: до h5.1.3.2578 build 20231110
QNAP QTS: до 5.1.3.2578 20231110

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

30 **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: 2024-01-08 / 2024-01-08

Ссылки на источник:

- http://www.qnap.com/en/security-advisory/qsa-23-22
- https://bdu.fstec.ru/vul/2023-00621

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-0225

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.130
Microsoft Edge: 79.0.309.71 - 120.0.2210.91

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

31

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html
- http://crbug.com/1506923
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0225

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-0224

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.130
Microsoft Edge: 79.0.309.71 - 120.0.2210.91

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.

32

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html
- http://crbug.com/1505086
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0224

33

Краткое описание: Отказ в обслуживании в HPE Unified OSS Console Assurance Monitoring (UOCAM)

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: HPE Unified OSS Console (UOC): до 3.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04570en_us
- https://bdu.fstec.ru/vul/2023-06559

34

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-0223

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.130
Microsoft Edge: 79.0.309.71 - 120.0.2210.91

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html
- http://crbug.com/1505009
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0223

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-0222

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 120.0.6099.130
Microsoft Edge: 79.0.309.71 - 120.0.2210.91

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: выполнение произвольного кода

35

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html
- http://crbug.com/1501798
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0222

36

Краткое описание: Выполнение произвольного кода в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2022-32231

Идентификатор программной ошибки: CWE-665 Некорректная инициализация

Уязвимый продукт: PowerScale OneFS: до 12.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities

37

Краткое описание: Отказ в обслуживании в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2022-4450

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: PowerScale OneFS: до 12.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 2024-01-05 / 2024-01-05

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-02240

38

Краткое описание: Отказ в обслуживании в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2023-0215

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PowerScale OneFS: до 12.0

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: 2024-01-05 / 2024-01-05

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2023-00675

Краткое описание: Выполнение произвольного кода в Hyland Alfresco Community Edition

Идентификатор уязвимости: CVE-2023-49964

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

Уязвимый продукт: Alfresco Community: 7.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

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: 2024-01-05 / 2024-01-05

Ссылки на источник:

- http://www.alfresco.com/products/community/download
- http://github.com/mbadanoiu/CVE-2023-49964

40

Краткое описание: Выполнение произвольного кода в Linux Mint Xreader

Идентификатор уязвимости: CVE-2023-44452

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Xreader: 1.0.1 - 3.8.4

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: 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: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1836/
- http://github.com/linuxmint/xreader/commit/cd678889ecfe4e84a5cbcf3a0489e15a5e2e3736

41

Краткое описание: Получение конфиденциальной информации в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2021-3712

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PowerScale OneFS: до 12.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 7.4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2021-04571

42

Краткое описание: Выполнение произвольного кода в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2021-3711

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

Уязвимый продукт: PowerScale OneFS: до 12.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-01-05 / 2024-01-05

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2021-04570

43

Краткое описание: Чтение локальных файлов в Linux Mint Xreader

Идентификатор уязвимости: CVE-2023-44451

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Xreader: 1.0.1 - 3.8.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: чтение локальных файлов

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

Оценка CVSSv3: 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: 2024-01-04 / 2024-01-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1835/
- http://github.com/linuxmint/xreader/commit/141f1313745b9cc73670df51ac145165efcbb14a
- https://bdu.fstec.ru/vul/2023-09145

Краткое описание: Отказ в обслуживании в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2022-0778

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

Уязвимый продукт: PowerScale OneFS: до 12.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

44 **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: 2024-01-05 / 2024-01-05

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000220650/dsa-2023-459-security-update-for-dell-powerscale-onefs-for-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2022-01315