НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-02-16.1 | 16 февраля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-0565	Linux kernel SMB client	Смежная сеть	ACE	2024-02-16	✓
2	Высокая	CVE-2023-49125	Siemens Parasolid	Локальный	OSI	2024-02-15	✓
3	Высокая	CVE-2024-23804	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
4	Высокая	CVE-2024-23802	Siemens Tecnomatix Plant Simulation	Локальный	OSI	2024-02-14	✓
5	Высокая	CVE-2024-23798	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
6	Высокая	CVE-2024-23797	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
7	Высокая	CVE-2024-23803	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
8	Высокая	CVE-2024-23796	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
9	Высокая	CVE-2024-23795	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-02-14	✓
10	Высокая	CVE-2024-24925	Siemens Simcenter Femap	Локальный	ACE	2024-02-14	✓
11	Высокая	CVE-2024-24924	Siemens Simcenter Femap	Локальный	ACE	2024-02-14	✓
12	Высокая	CVE-2024-24923	Siemens Simcenter Femap	Локальный	OSI	2024-02-14	✓
13	Высокая	CVE-2024-24922	Siemens Simcenter Femap	Локальный	ACE	2024-02-14	✓

14	Высокая	CVE-2024-24921	Siemens Simcenter Femap	Локальный	ACE	2024-02-14	✓
15	Высокая	CVE-2024-24920	Siemens Simcenter Femap	Локальный	ACE	2024-02-14	✓
16	Критическая	CVE-2024-21413	Microsoft Outlook	Сетевой	ACE	2024-02-13	✓
17	Высокая	CVE-2024-21378	Microsoft Outlook	Сетевой	ACE	2024-02-13	✓
18	Высокая	CVE-2024-20744	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
19	Высокая	CVE-2024-20743	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
20	Высокая	CVE-2024-20742	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
21	Высокая	CVE-2024-20741	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
22	Высокая	CVE-2024-20740	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
23	Высокая	CVE-2024-20723	Adobe Substance 3D Painter	Локальный	ACE	2024-02-13	✓
24	Критическая	CVE-2024-21376	Microsoft Azure Kubernetes Service Confidential Container	Сетевой	ACE	2024-02-13	✓
25	Критическая	CVE-2024-21403	Microsoft Azure Kubernetes Service Confidential Container	Сетевой	PE	2024-02-13	✓
26	Высокая	CVE-2024-20731	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓
27	Высокая	CVE-2024-20730	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓
28	Высокая	CVE-2024-20729	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓

29	Высокая	CVE-2024-20728	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓
30	Высокая	CVE-2024-20727	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓
31	Высокая	CVE-2024-20726	Adobe Acrobat and Reader	Локальный	ACE	2024-02-13	✓
32	Высокая	CVE-2024-21369	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
33	Высокая	CVE-2024-21361	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
34	Высокая	CVE-2024-21420	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
35	Высокая	CVE-2024-21366	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
36	Высокая	CVE-2024-21369	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
37	Высокая	CVE-2024-21352	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
38	Высокая	CVE-2024-21361	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
39	Высокая	CVE-2024-21367	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
40	Высокая	CVE-2024-21420	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
41	Высокая	CVE-2024-21370	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓

42	Высокая	CVE-2024-21366	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
43	Высокая	CVE-2024-21359	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
44	Высокая	CVE-2024-21352	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
45	Высокая	CVE-2024-21365	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
46	Высокая	CVE-2024-21367	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
47	Высокая	CVE-2024-21375	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
48	Высокая	CVE-2024-21370	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
49	Высокая	CVE-2024-21391	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
50	Высокая	CVE-2024-21359	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
51	Высокая	CVE-2024-21368	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
52	Высокая	CVE-2024-21365	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
53	Высокая	CVE-2024-21350	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓

54	Высокая	CVE-2024-21375	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
55	Высокая	CVE-2024-21360	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
56	Высокая	CVE-2024-21391	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
57	Высокая	CVE-2024-21358	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
58	Высокая	CVE-2024-21368	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
59	Высокая	CVE-2024-21350	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
60	Высокая	CVE-2024-21360	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
61	Высокая	CVE-2024-21358	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-02-13	✓
62	Высокая	CVE-2023-44487	HashiCorp Consul	Сетевой	DoS	2024-02-15	✓
63	Высокая	CVE-2024-23327	HashiCorp Consul	Сетевой	DoS	2024-02-15	✓
64	Высокая	CVE-2024-23322	HashiCorp Consul	Сетевой	DoS	2024-02-15	✓
65	Высокая	CVE-2024-23325	HashiCorp Consul	Сетевой	DoS	2024-02-15	✓
66	Высокая	CVE-2024-23324	HashiCorp Consul	Сетевой	SB	2024-02-15	✓

67	Критическая	CVE-2023-45614	Siemens Scalance W1750D	Сетевой	ACE	2024-02-14	✗
68	Критическая	CVE-2023-45615	Siemens Scalance W1750D	Сетевой	ACE	2024-02-14	✗
69	Критическая	CVE-2023-45616	Siemens Scalance W1750D	Сетевой	ACE	2024-02-14	✗
70	Высокая	CVE-2023-45617	Siemens Scalance W1750D	Сетевой	OAF	2024-02-14	✗
71	Высокая	CVE-2023-45618	Siemens Scalance W1750D	Сетевой	OAF	2024-02-14	✗
72	Высокая	CVE-2023-45619	Siemens Scalance W1750D	Сетевой	OAF	2024-02-14	✗
73	Высокая	CVE-2023-45620	Siemens Scalance W1750D	Сетевой	DoS	2024-02-14	✗
74	Высокая	CVE-2023-45622	Siemens Scalance W1750D	Сетевой	DoS	2024-02-14	✗
75	Высокая	CVE-2023-45623	Siemens Scalance W1750D	Сетевой	DoS	2024-02-14	✗
76	Высокая	CVE-2023-45624	Siemens Scalance W1750D	Сетевой	DoS	2024-02-14	✗
77	Высокая	CVE-2023-45621	Siemens Scalance W1750D	Сетевой	DoS	2024-02-14	✗
78	Критическая	CVE-2024-23816	Siemens Location Intelligence	Сетевой	ACE	2024-02-14	✓
79	Высокая	CVE-2024-21384	Microsoft Office OneNote	Локальный	ACE	2024-02-13	✓
80	Высокая	CVE-2024-20673	Microsoft Office	Локальный	ACE	2024-02-13	✓
81	Высокая	CVE-2024-21379	Microsoft Word	Локальный	ACE	2024-02-13	✓

82	Высокая	CVE-2024-20750	Adobe Substance 3D Designer	Сетевой	ACE	2024-02-13	✓
83	Критическая	CVE-2024-20738	Adobe FrameMaker Publishing Server	Сетевой	SB	2024-02-13	✓
84	Высокая	CVE-2024-20739	Adobe Audition	Сетевой	ACE	2024-02-13	✓
85	Высокая	CVE-2024-21353	Microsoft WDAC ODBC Driver	Сетевой	ACE	2024-02-13	✓
86	Высокая	CVE-2024-21349	Microsoft ActiveX Data Objects	Сетевой	ACE	2024-02-13	✓
87	Критическая	CVE-2024-21401	Microsoft Entra Jira Single-Sign-On Plugin	Сетевой	PE	2024-02-13	✓
88	Критическая	CVE-2024-24691	Zoom client for Windows	Сетевой	ACE	2024-02-14	✓
89	Критическая	CVE-2024-21410	Microsoft Exchange Server	Сетевой	OSI	2024-02-13	✓
90	Высокая	CVE-2024-21412	Microsoft Windows	Сетевой	ACE	2024-02-13	✓
91	Высокая	CVE-2024-21351	Microsoft Windows SmartScreen	Сетевой	ACE	2024-02-13	✓
92	Высокая	CVE-2024-21372	Microsoft Windows OLE	Сетевой	ACE	2024-02-13	✓
93	Высокая	None	Autodesk AutoCAD	Сетевой	ACE	2024-02-13	✗
94	Критическая	CVE-2023-51437	SASL token signature verification in Apache Pulsar	Сетевой	SB	2024-02-12	✓
95	Высокая	CVE-2023-31032	NVIDIA DGX Station A100 and DGX Station A800	Локальный	DoS	2024-02-09	✓

96	Высокая	CVE-2023-25521	NVIDIA DGX Station A100 and DGX Station A800	Локальный	PE	2024-02-09	✓

1

Краткое описание: Выполнение произвольного кода в Linux kernel SMB client

Идентификатор уязвимости: CVE-2024-0565

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Linux kernel: до 6.7 rc6

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

Способ эксплуатации: Подключение к вредоносному SMB-серверу

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-16 / 2024-02-16

Ссылки на источник:

- http://access.redhat.com/security/cve/CVE-2024-0565
- http://bugzilla.redhat.com/show_bug.cgi?id=2258518
- http://www.spinics.net/lists/stable-commits/msg328851.html
- https://bdu.fstec.ru/vul/2024-00581

2

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2023-49125

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: 35.0 - 36.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-797296.html

3

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23804

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

4

Краткое описание: Получение конфиденциальной информации в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23802

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

5

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23798

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

6

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23797

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23803

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

8

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23796

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

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-23795

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tecnomatix Plant Simulation: до 2302.0006

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

9 **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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-017796.html

10

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24925

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Simcenter Femap: до 2306.0000

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

11

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24924

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Simcenter Femap: до 2306.0000

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

12

Краткое описание: Получение конфиденциальной информации в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24923

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap: до 2401.0000

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

13

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24922

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Simcenter Femap: до 2401.0000

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

14

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24921

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

Уязвимый продукт: Simcenter Femap: до 2401.0000

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 7.8 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2024-24920

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Simcenter Femap: до 2401.0000

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-000072.html

Краткое описание: Выполнение произвольного кода в Microsoft Outlook

Идентификатор уязвимости: CVE-2024-21413

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: выполнение произвольного кода

16

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413
- https://bdu.fstec.ru/vul/2024-01322

17

Краткое описание: Выполнение произвольного кода в Microsoft Outlook

Идентификатор уязвимости: CVE-2024-21378

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Outlook: 2016 - 2019
Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions
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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378

18

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

Идентификатор уязвимости: CVE-2024-20744

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

19

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

Идентификатор уязвимости: CVE-2024-20743

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

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

Идентификатор уязвимости: CVE-2024-20742

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

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

Идентификатор уязвимости: CVE-2024-20741

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

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

Идентификатор уязвимости: CVE-2024-20740

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

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

Идентификатор уязвимости: CVE-2024-20723

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

Уязвимый продукт: Substance 3D Painter: 2.2 - 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 7.8 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html

Краткое описание: Выполнение произвольного кода в Microsoft Azure Kubernetes Service Confidential Container

Идентификатор уязвимости: CVE-2024-21376

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Azure Kubernetes Service Confidential Containers: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21376

Краткое описание: Повышение привилегий в Microsoft Azure Kubernetes Service Confidential Container

Идентификатор уязвимости: CVE-2024-21403

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Azure Kubernetes Service Confidential Containers: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21403

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20731

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20730

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

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

27

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

Оценка CVSSv3: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20729

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20728

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20727

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-20726

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 23.008.20470
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-07.html

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21369

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21369

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21361

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

33

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21361

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21420

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

34

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21420

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21366

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21366

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21369

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

36

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21369

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21352

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

37

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21352

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21361

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

38

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21361

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21367

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

39

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21367

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21420

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

40

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21420

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21370

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

41 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21370

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21366

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

42 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21366

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21359

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

43 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21359

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21352

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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: 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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21352

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21365

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

45

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21365

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21367

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

46

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21367

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21375

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

47

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21375

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21370

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

48 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21370

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21391

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

49

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21391

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21359

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

50

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21359

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21368

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

51

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21368

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21365

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

52

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21365

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21350

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

53 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21350

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21375

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

54

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21375

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21360

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

55

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21360

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21391

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

56

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21391

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21358

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

57

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21358

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21368

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

58

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21368

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21350

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

59

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21350

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21360

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

60

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21360

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-21358

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

61

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21358

62

Краткое описание: Отказ в обслуживании в HashiCorp Consul

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Consul Enterprise: 1.0.0 - 1.17.2

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.6
- http://github.com/hashicorp/consul/releases/tag/v1.15.10
- https://bdu.fstec.ru/vul/2023-06559

63

Краткое описание: Отказ в обслуживании в HashiCorp Consul

Идентификатор уязвимости: CVE-2024-23327

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Consul Enterprise: 1.0.0 - 1.17.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.6
- http://github.com/hashicorp/consul/releases/tag/v1.15.10

64

Краткое описание: Отказ в обслуживании в HashiCorp Consul

Идентификатор уязвимости: CVE-2024-23322

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Consul Enterprise: 1.0.0 - 1.17.2

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.6
- http://github.com/hashicorp/consul/releases/tag/v1.15.10

65

Краткое описание: Отказ в обслуживании в HashiCorp Consul

Идентификатор уязвимости: CVE-2024-23325

Идентификатор программной ошибки: CWE-248 Необработанное исключение

Уязвимый продукт: Consul Enterprise: 1.0.0 - 1.17.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.6
- http://github.com/hashicorp/consul/releases/tag/v1.15.10

66

Краткое описание: Обход безопасности в HashiCorp Consul

Идентификатор уязвимости: CVE-2024-23324

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Consul Enterprise: 1.0.0 - 1.17.2

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-15 / 2024-02-15

Ссылки на источник:

- http://github.com/hashicorp/consul/releases/tag/v1.16.6
- http://github.com/hashicorp/consul/releases/tag/v1.15.10

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45614

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

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

67 **Последствия эксплуатации:** выполнение произвольного кода

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

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45615

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

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

68 **Последствия эксплуатации:** выполнение произвольного кода

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

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45616

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

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

69 **Последствия эксплуатации:** выполнение произвольного кода

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

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Перезапись произвольных файлов в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45617

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

70 **Последствия эксплуатации:** перезапись произвольных файлов

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Перезапись произвольных файлов в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45618

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

71 **Последствия эксплуатации:** перезапись произвольных файлов

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Перезапись произвольных файлов в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45619

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

72 **Последствия эксплуатации:** перезапись произвольных файлов

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Отказ в обслуживании в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45620

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

73 **Последствия эксплуатации:** отказ в обслуживании

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

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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Отказ в обслуживании в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45622

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

74 **Последствия эксплуатации:** отказ в обслуживании

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

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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Отказ в обслуживании в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45623

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

75 **Последствия эксплуатации:** отказ в обслуживании

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

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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Отказ в обслуживании в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45624

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

76 **Последствия эксплуатации:** отказ в обслуживании

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

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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Отказ в обслуживании в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-45621

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SCALANCE W1750D (JP): все версии
SCALANCE W1750D (ROW): все версии
SCALANCE W1750D (USA): все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

77 **Последствия эксплуатации:** отказ в обслуживании

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

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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-716164.txt

Краткое описание: Выполнение произвольного кода в Siemens Location Intelligence

Идентификатор уязвимости: CVE-2024-23816

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

Уязвимый продукт: Location Intelligence Perpetual Large: до 4.3
Location Intelligence Perpetual Medium: до 4.3
Location Intelligence Perpetual Non-Prod: до 4.3
Location Intelligence Perpetual Small: до 4.3
Location Intelligence SUS Large: до 4.3
Location Intelligence SUS Medium: до 4.3
Location Intelligence SUS Non-Prod: до 4.3
Location Intelligence SUS Small: до 4.3

Категория уязвимого продукта: Телекоммуникационное оборудование

78 **Способ эксплуатации:** Использование жестко закодированных учетных 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: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-580228.html
- https://bdu.fstec.ru/vul/2024-01288

Краткое описание: Выполнение произвольного кода в Microsoft Office OneNote

Идентификатор уязвимости: CVE-2024-21384

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions
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

79

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384

80

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2024-20673

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office: 2016 - 2019
Microsoft Excel: 2016
Microsoft PowerPoint: 2016
Microsoft Visio: 2016
Microsoft Word: 2016
Microsoft Publisher: 2016
Skype for Business: 2016
Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2024-21379

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office: 2019
Microsoft Word: 2016
Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions
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.

81 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379

82

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

Идентификатор уязвимости: CVE-2024-20750

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Substance 3D Designer: 10.1.0 - 13.1.0

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb24-13.html

83

Краткое описание: Обход безопасности в Adobe FrameMaker Publishing Server

Идентификатор уязвимости: CVE-2024-20738

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe Framemaker: 2017.0 - 2022.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-10.html

84

Краткое описание: Выполнение произвольного кода в Adobe Audition

Идентификатор уязвимости: CVE-2024-20739

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

Уязвимый продукт: Adobe Audition: 23.6.0 - 24.0.3

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/audition/apsb24-11.html

Краткое описание: Выполнение произвольного кода в Microsoft WDAC ODBC Driver

Идентификатор уязвимости: CVE-2024-21353

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: 2019 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

85 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21353

Краткое описание: Выполнение произвольного кода в Microsoft ActiveX Data Objects

Идентификатор уязвимости: CVE-2024-21349

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

86

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21349

Краткое описание: Повышение привилегий в Microsoft Entra Jira Single-Sign-On Plugin

Идентификатор уязвимости: CVE-2024-21401

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Microsoft Entra Jira Single-Sign-On Plugin: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: повышение привилегий

87 **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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21401

Краткое описание: Выполнение произвольного кода в Zoom client for Windows

Идентификатор уязвимости: CVE-2024-24691

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Zoom Client for Windows: 5.0.0 23168.0427 - 5.16.2 22807
Virtual Desktop Infrastructure (VDI): 5.0.1 - 5.16.0 24280
Zoom Meeting SDK for Windows: 5.9.0 - 5.16.2
Zoom Rooms for Windows: 5.0.0 1420.0426 - 5.16.10 3425

Категория уязвимого продукта: Прикладное программное обеспечение

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

88 **Последствия эксплуатации:** выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-14 / 2024-02-14

Ссылки на источник:

- http://www.zoom.com/en/trust/security-bulletin/ZSB-24008/

89

Краткое описание: Получение конфиденциальной информации в Microsoft Exchange Server

Идентификатор уязвимости: CVE-2024-21410

Идентификатор программной ошибки: CWE-668 Возможность несанкционированного доступа к ресурсу

Уязвимый продукт: Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21410

Краткое описание: Выполнение произвольного кода в Microsoft Windows

Идентификатор уязвимости: CVE-2024-21412

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2019 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

90

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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21412

Краткое описание: Выполнение произвольного кода в Microsoft Windows SmartScreen

Идентификатор уязвимости: CVE-2024-21351

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2016 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: выполнение произвольного кода

91 **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: 7.6 AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21351
- https://bdu.fstec.ru/vul/2024-01289

Краткое описание: Выполнение произвольного кода в Microsoft Windows OLE

Идентификатор уязвимости: CVE-2024-21372

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

92

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: 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21372

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD

Идентификатор уязвимости: None

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

Уязвимый продукт: Autodesk AutoCAD: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

93 **Дата выявления / Дата обновления:** 2024-02-13 / 2024-02-13

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-145/
- http://www.zerodayinitiative.com/advisories/ZDI-24-143/
- http://www.zerodayinitiative.com/advisories/ZDI-24-142/
- http://www.zerodayinitiative.com/advisories/ZDI-24-141/
- http://www.zerodayinitiative.com/advisories/ZDI-24-140/
- http://www.zerodayinitiative.com/advisories/ZDI-24-139/
- http://www.zerodayinitiative.com/advisories/ZDI-24-138/
- http://www.zerodayinitiative.com/advisories/ZDI-24-137/
- http://www.zerodayinitiative.com/advisories/ZDI-24-136/
- http://www.zerodayinitiative.com/advisories/ZDI-24-135/
- http://www.zerodayinitiative.com/advisories/ZDI-24-134/
- http://www.zerodayinitiative.com/advisories/ZDI-24-133/
- http://www.zerodayinitiative.com/advisories/ZDI-24-132/
- http://www.zerodayinitiative.com/advisories/ZDI-24-131/
- http://www.zerodayinitiative.com/advisories/ZDI-24-130/

- http://www.zerodayinitiative.com/advisories/ZDI-24-129/
- http://www.zerodayinitiative.com/advisories/ZDI-24-128/
- http://www.zerodayinitiative.com/advisories/ZDI-24-127/
- http://www.zerodayinitiative.com/advisories/ZDI-24-126/
- http://www.zerodayinitiative.com/advisories/ZDI-24-125/
- http://www.zerodayinitiative.com/advisories/ZDI-24-124/
- http://www.zerodayinitiative.com/advisories/ZDI-24-144/
- http://www.zerodayinitiative.com/advisories/ZDI-24-146/
- http://www.zerodayinitiative.com/advisories/ZDI-24-147/
- http://www.zerodayinitiative.com/advisories/ZDI-24-148/
- http://www.zerodayinitiative.com/advisories/ZDI-24-149/
- http://www.zerodayinitiative.com/advisories/ZDI-24-150/
- http://www.zerodayinitiative.com/advisories/ZDI-24-151/
- http://www.zerodayinitiative.com/advisories/ZDI-24-152/
- http://www.zerodayinitiative.com/advisories/ZDI-24-153/
- http://www.zerodayinitiative.com/advisories/ZDI-24-154/
- http://www.zerodayinitiative.com/advisories/ZDI-24-155/
- http://www.zerodayinitiative.com/advisories/ZDI-24-156/
- http://www.zerodayinitiative.com/advisories/ZDI-24-157/
- http://www.zerodayinitiative.com/advisories/ZDI-24-158/
- http://www.zerodayinitiative.com/advisories/ZDI-24-159/
- http://www.zerodayinitiative.com/advisories/ZDI-24-160/
- http://www.zerodayinitiative.com/advisories/ZDI-24-161/
- http://www.zerodayinitiative.com/advisories/ZDI-24-162/
- http://www.zerodayinitiative.com/advisories/ZDI-24-163/

94

Краткое описание: Обход безопасности в SASL token signature verification in Apache Pulsar

Идентификатор уязвимости: CVE-2023-51437

Идентификатор программной ошибки: CWE-203 Наблюдаемые различия в поведении в ответ на некорректный ввод

Уязвимый продукт: Apache Pulsar: 2.0.0 - 3.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-02-12 / 2024-02-12

Ссылки на источник:

- http://lists.apache.org/thread/5kgmvvolf5tzp5rz9xjwfg2ncwvqqgl5
- http://www.openwall.com/lists/oss-security/2024/02/07/1

Краткое описание: Отказ в обслуживании в NVIDIA DGX Station A100 and DGX Station A800

Идентификатор уязвимости: CVE-2023-31032

Идентификатор программной ошибки: CWE-627 Уязвимости, связанные с динамическими переменными

Уязвимый продукт: DGX Station A100: все версии
DGX Station A800: все версии
NVIDIA SBIOS: до 10.20

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

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

95

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: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://nvidia.custhelp.com/app/answers/detail/a_id/5513
- https://bdu.fstec.ru/vul/2024-00316

96

Краткое описание: Повышение привилегий в NVIDIA DGX Station A100 and DGX Station A800

Идентификатор уязвимости: CVE-2023-25521

Идентификатор программной ошибки: CWE-250 Выполнение операций с избыточными привилегиями

Уязвимый продукт: DGX Station A800: все версии
DGX Station A100: все версии
NVIDIA SBIOS: до 10.20

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 7.5 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: 2024-02-09 / 2024-02-09

Ссылки на источник:

- http://nvidia.custhelp.com/app/answers/detail/a_id/5513