НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-15.1 | 15 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-35272	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
2	Высокая	CVE-2024-21425	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
3	Высокая	CVE-2024-21331	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
4	Высокая	CVE-2024-21335	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
5	Высокая	CVE-2024-37336	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
6	Высокая	CVE-2024-28928	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
7	Высокая	CVE-2024-37319	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
8	Высокая	CVE-2024-20701	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
9	Высокая	CVE-2024-35271	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
10	Высокая	CVE-2024-21428	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓

11	Высокая	CVE-2024-35256	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
12	Высокая	CVE-2024-37320	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
13	Высокая	CVE-2024-37323	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
14	Высокая	CVE-2024-21308	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
15	Высокая	CVE-2024-37322	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
16	Высокая	CVE-2024-37333	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
17	Высокая	CVE-2024-21303	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
18	Высокая	CVE-2024-37331	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
19	Высокая	CVE-2024-37328	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
20	Высокая	CVE-2024-21317	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
21	Высокая	CVE-2024-21398	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
22	Высокая	CVE-2024-37321	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓

23	Высокая	CVE-2024-21415	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
24	Высокая	CVE-2024-38088	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
25	Высокая	CVE-2024-37330	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
26	Высокая	CVE-2024-37329	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
27	Высокая	CVE-2024-21373	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
28	Высокая	CVE-2024-37327	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
29	Высокая	CVE-2024-21333	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
30	Высокая	CVE-2024-37324	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
31	Высокая	CVE-2024-37332	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
32	Высокая	CVE-2024-37318	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
33	Высокая	CVE-2024-37326	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
34	Высокая	CVE-2024-21414	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓

35	Высокая	CVE-2024-38087	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
36	Высокая	CVE-2024-21332	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
37	Высокая	CVE-2024-21449	Microsoft SQL Server Native Client OLE DB Provider	Сетевой	ACE	2024-07-09	✓
38	Высокая	CVE-2024-37997	Siemens JT Open and PLM XML SDK	Локальный	ACE	2024-07-12	✓
39	Высокая	CVE-2024-5990	Rockwell Automation ThinManager, ThinServer	Сетевой	DoS	2024-07-12	✓
40	Критическая	CVE-2024-5989	Rockwell Automation ThinManager, ThinServer	Сетевой	ACE	2024-07-12	✓
41	Критическая	CVE-2024-5988	Rockwell Automation ThinManager, ThinServer	Сетевой	ACE	2024-07-12	✓
42	Высокая	CVE-2024-39883	Delta Electronics CNCSoft-G2	Сетевой	ACE	2024-07-10	✓
43	Высокая	CVE-2024-39882	Delta Electronics CNCSoft-G2	Сетевой	OSI	2024-07-10	✓
44	Высокая	CVE-2024-39881	Delta Electronics CNCSoft-G2	Сетевой	ACE	2024-07-10	✓
45	Высокая	CVE-2024-39880	Delta Electronics CNCSoft-G2	Локальный	ACE	2024-07-10	✓
46	Высокая	CVE-2024-39571	Siemens SINEMA Remote Connect Server	Сетевой	ACE	2024-07-11	✓
47	Высокая	CVE-2024-39570	Siemens SINEMA Remote Connect Server	Сетевой	ACE	2024-07-11	✓

48	Критическая	CVE-2024-34108	Adobe Commerce and Magento Open Source	Сетевой	ACE	2024-07-10	✓
49	Высокая	CVE-2024-34104	Adobe Commerce and Magento Open Source	Сетевой	SB	2024-07-10	✓
50	Высокая	CVE-2024-34103	Adobe Commerce and Magento Open Source	Сетевой	SB	2024-07-10	✓
51	Критическая	CVE-2024-34102	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2024-07-10	✓
52	Высокая	CVE-2024-38095	Microsoft .NET and Visual Studio	Сетевой	DoS	2024-07-10	✓
53	Высокая	CVE-2024-35264	Microsoft .NET and Visual Studio	Сетевой	ACE	2024-07-10	✓
54	Высокая	CVE-2024-20782	Adobe InDesign	Локальный	ACE	2024-07-09	✓
55	Высокая	CVE-2024-20785	Adobe InDesign	Локальный	ACE	2024-07-09	✓
56	Высокая	CVE-2024-20783	Adobe InDesign	Локальный	ACE	2024-07-09	✓
57	Высокая	CVE-2024-20781	Adobe InDesign	Локальный	ACE	2024-07-09	✓
58	Высокая	CVE-2024-34139	Adobe Bridge	Локальный	ACE	2024-07-09	✓
59	Высокая	CVE-2024-38051	Microsoft Windows Graphics Component	Локальный	ACE	2024-07-09	✓
60	Высокая	CVE-2024-38079	Microsoft Windows Graphics Component	Локальный	PE	2024-07-09	✓

61	Высокая	CVE-2024-38085	Microsoft Windows Graphics Component	Локальный	PE	2024-07-09	✓
62	Высокая	CVE-2024-38072	Microsoft Windows Remote Desktop Licensing Service	Сетевой	DoS	2024-07-09	✓
63	Критическая	CVE-2024-38077	Microsoft Windows Remote Desktop Licensing Service	Сетевой	ACE	2024-07-09	✓
64	Высокая	CVE-2024-38071	Microsoft Windows Remote Desktop Licensing Service	Сетевой	DoS	2024-07-09	✓
65	Критическая	CVE-2024-38076	Microsoft Windows Remote Desktop Licensing Service	Сетевой	ACE	2024-07-09	✓
66	Высокая	CVE-2024-38073	Microsoft Windows Remote Desktop Licensing Service	Сетевой	DoS	2024-07-09	✓
67	Критическая	CVE-2024-38074	Microsoft Windows Remote Desktop Licensing Service	Сетевой	ACE	2024-07-09	✓
68	Высокая	CVE-2024-39562	Juniper Junos OS Evolved	Сетевой	DoS	2024-07-15	✓
69	Высокая	CVE-2024-0107	NVIDIA GPU Display Driver	Сетевой	ACE	2024-07-15	✓
70	Высокая	CVE-2023-51794	FFmpeg	Сетевой	ACE	2024-07-11	✓
71	Высокая	CVE-2024-38517	Microsoft products	Локальный	ACE	2024-07-10	✓
72	Высокая	CVE-2024-39684	Microsoft products	Локальный	PE	2024-07-10	✓
73	Критическая	CVE-2024-34123	Adobe Premiere Pro	Сетевой	ACE	2024-07-09	✓

74	Высокая	CVE-2024-38021	Microsoft Office	Сетевой	ACE	2024-07-09	✓
75	Высокая	CVE-2024-37334	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-07-09	✓
76	Высокая	CVE-2024-38104	Microsoft Windows Fax Service	Сетевой	ACE	2024-07-09	✓
77	Высокая	CVE-2024-30013	Microsoft Windows MultiPoint Services	Сетевой	ACE	2024-07-09	✓
78	Высокая	CVE-2024-30013	Microsoft Windows MultiPoint Services	Сетевой	ACE	2024-07-09	✓
79	Высокая	CVE-2024-38080	Microsoft Windows Hyper-V	Локальный	ACE	2024-07-09	✓
80	Высокая	CVE-2024-38112	Windows MSHTML Platform	Сетевой	OSI	2024-07-09	✓
81	Высокая	CVE-2024-6604	Mozilla Firefox	Сетевой	ACE	2024-07-09	✓
82	Высокая	CVE-2024-6602	Mozilla Firefox	Сетевой	ACE	2024-07-09	✓
83	Высокая	CVE-2024-6600	Mozilla Firefox	Сетевой	ACE	2024-07-09	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-35272

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35272

2

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21425

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21425

3

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21331

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21331

4

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21335

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21335

5

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37336

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37336

6

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-28928

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28928

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37319

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37319

8

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-20701

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20701

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-35271

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35271

10

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21428

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21428

11

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-35256

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35256

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37320

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37320

13

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37323

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37323

14

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21308

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21308

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37322

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37322

16

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37333

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37333

17

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21303

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21303

18

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37331

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37331

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37328

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37328

20

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21317

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21317

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21398

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21398

22

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37321

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37321

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21415

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21415

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-38088

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38088

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37330

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37330

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37329

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37329

27

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21373

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21373

28

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37327

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37327

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21333

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21333

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37324

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37324

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37332

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37332

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37318

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37318

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-37326

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37326

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21414

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21414

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-38087

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38087

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21332

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21332

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server Native Client OLE DB Provider

Идентификатор уязвимости: CVE-2024-21449

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21449

Краткое описание: Выполнение произвольного кода в Siemens JT Open and PLM XML SDK

Идентификатор уязвимости: CVE-2024-37997

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: JT Open: до 11.5
PLM XML SDK: до 7.1.0.014

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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: 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: 2024-07-12 / 2024-07-12

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-824889.html

Краткое описание: Отказ в обслуживании в Rockwell Automation ThinManager, ThinServer

Идентификатор уязвимости: CVE-2024-5990

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ThinManager: 11.1.0 - 13.1.0
ThinServer: 11.1.0 - 13.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-12 / 2024-07-12

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-193-18

Краткое описание: Выполнение произвольного кода в Rockwell Automation ThinManager, ThinServer

Идентификатор уязвимости: CVE-2024-5989

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

Уязвимый продукт: ThinManager: 11.1.0 - 13.2.0
ThinServer: 11.1.0 - 13.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-07-12 / 2024-07-12

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-193-18
- https://bdu.fstec.ru/vul/2024-04810

41

Краткое описание: Выполнение произвольного кода в Rockwell Automation ThinManager, ThinServer

Идентификатор уязвимости: CVE-2024-5988

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ThinManager: 11.1.0 - 13.2.0
ThinServer: 11.1.0 - 13.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-12 / 2024-07-12

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1677.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-193-18
- https://bdu.fstec.ru/vul/2024-05060

42

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

Идентификатор уязвимости: CVE-2024-39883

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

Уязвимый продукт: CNCSoft-G2: 2.0.0.5

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: 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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

43

Краткое описание: Получение конфиденциальной информации в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2024-39882

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: CNCSoft-G2: 2.0.0.5

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: 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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

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

Идентификатор уязвимости: CVE-2024-39881

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: CNCSoft-G2: 2.0.0.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

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

Идентификатор уязвимости: CVE-2024-39880

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CNCSoft-G2: 2.0.0.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

Краткое описание: Выполнение произвольного кода в Siemens SINEMA Remote Connect Server

Идентификатор уязвимости: CVE-2024-39571

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

Уязвимый продукт: SINEMA Remote Connect Server: до 3.2 HF1

Категория уязвимого продукта: Серверное программное обеспечение и его 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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-11 / 2024-07-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-928781.html

Краткое описание: Выполнение произвольного кода в Siemens SINEMA Remote Connect Server

Идентификатор уязвимости: CVE-2024-39570

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

Уязвимый продукт: SINEMA Remote Connect Server: до 3.2 HF1

Категория уязвимого продукта: Серверное программное обеспечение и его 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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-11 / 2024-07-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-928781.html

Краткое описание: Выполнение произвольного кода в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-34108

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.0.0 - 2.4.7-beta2
Magento Open Source: 2.0.0 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://bdu.fstec.ru/vul/2024-04664

Краткое описание: Обход безопасности в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-34104

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.0.0 - 2.4.7-beta2
Magento Open Source: 2.0.0 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://bdu.fstec.ru/vul/2024-04665

Краткое описание: Обход безопасности в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-34103

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.0.0 - 2.4.7-beta2
Magento Open Source: 2.0.0 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://bdu.fstec.ru/vul/2024-04654

Краткое описание: Межсайтовый скриптинг в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-34102

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.0.0 - 2.4.7-beta2
Magento Open Source: 2.0.0 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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: 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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://bdu.fstec.ru/vul/2024-04655

Краткое описание: Отказ в обслуживании в Microsoft .NET and Visual Studio

Идентификатор уязвимости: CVE-2024-38095

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Visual Studio: 2022 version 17.4 - 2022 version 17.10
.NET: 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095

Краткое описание: Выполнение произвольного кода в Microsoft .NET and Visual Studio

Идентификатор уязвимости: CVE-2024-35264

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Visual Studio: 2022 version 17.4 - 2022 version 17.10
.NET: 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35264

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-20782

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: 18.0 - 19.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-48.html

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-20785

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

Уязвимый продукт: Adobe InDesign: 18.0 - 19.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-48.html

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-20783

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

Уязвимый продукт: Adobe InDesign: 18.0 - 19.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-48.html

57

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-20781

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

Уязвимый продукт: Adobe InDesign: 18.0 - 19.3

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-48.html

58

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2024-34139

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

Уязвимый продукт: Adobe Bridge: 13.0 - 14.1.0

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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/bridge/apsb24-51.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Graphics Component

Идентификатор уязвимости: CVE-2024-38051

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38051

Краткое описание: Повышение привилегий в Microsoft Windows Graphics Component

Идентификатор уязвимости: CVE-2024-38079

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Выполнение специально созданного вредоносного файла

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38079

Краткое описание: Повышение привилегий в Microsoft Windows Graphics Component

Идентификатор уязвимости: CVE-2024-38085

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38085

Краткое описание: Отказ в обслуживании в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38072

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

62 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38072

63

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38077

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

Категория уязвимого продукта: Unix-подобные операционные системы 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: 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38077

64

Краткое описание: Отказ в обслуживании в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38071

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38071

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38076

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

65 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38076

66

Краткое описание: Отказ в обслуживании в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38073

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38073

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Desktop Licensing Service

Идентификатор уязвимости: CVE-2024-38074

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

67 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38074

Краткое описание: Отказ в обслуживании в Juniper Junos OS Evolved

Идентификатор уязвимости: CVE-2024-39562

Идентификатор программной ошибки: CWE-772 Удержание ресурса после его использования

Уязвимый продукт: Junos OS Evolved: 21.4R1-EVO - 23.2R1-S2-EVO

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

68 **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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://supportportal.juniper.net/JSA75724

Краткое описание: Выполнение произвольного кода в NVIDIA GPU Display Driver

Идентификатор уязвимости: CVE-2024-0107

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: R555: до 556.12
R470: до 475.14
R550: до 552.74
R535: до 538.78

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

69 **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: 2024-07-15 / 2024-07-15

Ссылки на источник:

- http://nvidia.custhelp.com/app/answers/detail/a_id/5557

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51794

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

Уязвимый продукт: FFmpeg: 6.0 - 6.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

70 **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: 2024-07-11 / 2024-07-11

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10746
- http://git.videolan.org/?p=ffmpeg.git;a=commitdiff;h=50f0f8c53c818f73fe2d752708e2fa9d2a2d8a07

Краткое описание: Выполнение произвольного кода в Microsoft products

Идентификатор уязвимости: CVE-2024-38517

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

71 **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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38517
- http://github.com/Tencent/rapidjson/pull/1261/commits/8269bc2bc289e9d343bae51cdf6d23ef0950e001
- http://github.com/fmalita/rapidjson/commit/8269bc2bc289e9d343bae51cdf6d23ef0950e001

Краткое описание: Повышение привилегий в Microsoft products

Идентификатор уязвимости: CVE-2024-39684

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Повышение привилегий

72

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: 2024-07-10 / 2024-07-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-39684

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2024-34123

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Premiere Pro: 23.6.2 - 24.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/premiere_pro/apsb24-46.html

74

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2024-38021

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: 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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021

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

Идентификатор уязвимости: CVE-2024-37334

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

Уязвимый продукт: Microsoft SQL Server: до 2022 CU13 16.0.4131.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

75 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37334

Краткое описание: Выполнение произвольного кода в Microsoft Windows Fax Service

Идентификатор уязвимости: CVE-2024-38104

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

76

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104

77

Краткое описание: Выполнение произвольного кода в Microsoft Windows MultiPoint Services

Идентификатор уязвимости: CVE-2024-30013

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

Категория уязвимого продукта: Unix-подобные операционные системы 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: 8.8 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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30013

Краткое описание: Выполнение произвольного кода в Microsoft Windows MultiPoint Services

Идентификатор уязвимости: CVE-2024-30013

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

78 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30013

Краткое описание: Выполнение произвольного кода в Microsoft Windows Hyper-V

Идентификатор уязвимости: CVE-2024-38080

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2582
Windows: до 11 23H2 10.0.22631.3880

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38080
- https://bdu.fstec.ru/vul/2024-05135

Краткое описание: Получение конфиденциальной информации в Windows MSHTML Platform

Идентификатор уязвимости: CVE-2024-38112

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

Уязвимый продукт: Microsoft Internet Explorer: 11 - 11.1790.17763.0
Windows: до 11 23H2 10.0.22631.3880
Windows Server: до 2022 10.0.20348.2582

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

80

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38112
- https://bdu.fstec.ru/vul/2024-05134

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-6604

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

Уязвимый продукт: Firefox ESR: 102.0 - 115.12.0
Mozilla Firefox: 100.0 - 127.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

81 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-30/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-29/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-6602

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

Уязвимый продукт: Firefox ESR: 102.0 - 115.12.0
Mozilla Firefox: 100.0 - 127.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

82 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-30/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-29/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-6600

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

Уязвимый продукт: Firefox ESR: 102.0 - 115.12.0
Mozilla Firefox: 100.0 - 127.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

83 **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: 2024-07-09 / 2024-07-09

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-30/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-29/