НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-04-12.1 | 12 апреля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-2757	PHP	Сетевой	DoS	2024-04-11	✓
2	Критическая	CVE-2024-3096	PHP	Сетевой	SB	2024-04-11	✓
3	Высокая	cve-2024-20314	Cisco IOS XE	Сетевой	DoS	2024-03-27	✓
4	Высокая	cve-2024-20311	Cisco IOS XE	Сетевой	DoS	2024-03-27	✓
5	Критическая	cve-2024-28288	Ruijie RG-NBR700GW	Сетевой	SB	2024-03-30	✗
6	Высокая	CVE-2024-26275	Siemens Parasolid	Локальный	OSI	2024-04-11	✓
7	Критическая	CVE-2023-35982	Siemens Scalance W1750D	Сетевой	ACE	2024-04-11	✓
8	Высокая	CVE-2024-3515	Google Chrome	Сетевой	ACE	2024-04-10	✓
9	Критическая	CVE-2023-35981	Siemens Scalance W1750D	Сетевой	ACE	2024-04-11	✓
10	Критическая	CVE-2023-35980	Siemens Scalance W1750D	Сетевой	ACE	2024-04-11	✓
11	Не определено	CVE-2024-3516	Google Chrome	Не определено	ACE	2024-04-10	✓
12	Высокая	CVE-2024-3157	Google Chrome	Сетевой	ACE	2024-04-10	✓
13	Высокая	CVE-2024-20670	Microsoft Outlook for Windows	Сетевой	XSS\CSS	2024-04-10	✓

14	Высокая	CVE-2024-26214	Microsoft WDAC SQL Server ODBC Driver	Сетевой	ACE	2024-04-10	✓
15	Высокая	CVE-2024-26256	Microsoft Windows libarchive	Сетевой	ACE	2024-04-10	✓
16	Высокая	CVE-2024-26234	Microsoft Windows proxy driver	Локальный	ACE	2024-04-10	✓
17	Высокая	CVE-2024-26257	Microsoft Excel	Локальный	ACE	2024-04-10	✓
18	Критическая	CVE-2024-29990	Microsoft Azure Kubernetes Service Confidential Container	Сетевой	PE	2024-04-10	✓
19	Критическая	CVE-2024-24576	Rust	Сетевой	ACE	2024-04-10	✓
20	Высокая	CVE-2024-26210	Microsoft WDAC OLE DB Provider for SQL Server	Сетевой	ACE	2024-04-10	✓
21	Высокая	CVE-2024-26244	Microsoft WDAC OLE DB Provider for SQL Server	Сетевой	ACE	2024-04-10	✓
22	Высокая	CVE-2024-26228	Microsoft Windows Cryptographic Services	Локальный	OSI	2024-04-10	✓
23	Высокая	CVE-2024-29050	Microsoft Windows Cryptographic Services	Локальный	ACE	2024-04-10	✓
24	Высокая	CVE-2024-29988	Microsoft Windows	Сетевой	SB	2024-04-09	✓
25	Высокая	CVE-2024-28938	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
26	Высокая	CVE-2024-28941	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
27	Высокая	CVE-2024-29043	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓

28	Высокая	CVE-2024-28935	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
29	Высокая	CVE-2024-28936	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
30	Высокая	CVE-2024-28931	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
31	Высокая	CVE-2024-28929	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
32	Высокая	CVE-2024-28937	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
33	Высокая	CVE-2024-28943	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
34	Высокая	CVE-2024-28932	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
35	Высокая	CVE-2024-28930	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
36	Высокая	CVE-2024-28933	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
37	Высокая	CVE-2024-28934	Microsoft ODBC Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
38	Высокая	CVE-2024-20759	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2024-04-09	✓
39	Критическая	CVE-2024-20758	Adobe Commerce and Magento Open Source	Сетевой	ACE	2024-04-09	✓
40	Высокая	CVE-2024-20772	Adobe Media Encoder	Локальный	ACE	2024-04-09	✓
41	Высокая	CVE-2024-20795	Adobe Animate	Локальный	ACE	2024-04-09	✓
42	Высокая	CVE-2024-20797	Adobe Animate	Локальный	RLF	2024-04-09	✓

43	Высокая	CVE-2024-29044	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
44	Высокая	CVE-2024-28913	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
45	Высокая	CVE-2024-28915	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
46	Высокая	CVE-2024-28912	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
47	Высокая	CVE-2024-28909	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
48	Высокая	CVE-2024-28944	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
49	Высокая	CVE-2024-29982	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
50	Высокая	CVE-2024-28914	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
51	Высокая	CVE-2024-28939	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
52	Высокая	CVE-2024-28908	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
53	Высокая	CVE-2024-28926	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
54	Высокая	CVE-2024-28906	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
55	Высокая	CVE-2024-29984	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
56	Высокая	CVE-2024-28911	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
57	Высокая	CVE-2024-29045	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓

58	Высокая	CVE-2024-28927	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
59	Высокая	CVE-2024-28910	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
60	Высокая	CVE-2024-29046	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
61	Высокая	CVE-2024-29048	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
62	Высокая	CVE-2024-28942	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
63	Высокая	CVE-2024-28945	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
64	Высокая	CVE-2024-29985	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
65	Высокая	CVE-2024-29983	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
66	Высокая	CVE-2024-29047	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
67	Высокая	CVE-2024-28940	Microsoft OLE DB Driver for SQL Server	Сетевой	ACE	2024-04-09	✓
68	Критическая	CVE-2023-45590	FortiClient for Linux	Сетевой	ACE	2024-04-09	✓
69	Критическая	CVE-2024-3272	D-Link routers	Сетевой	ACE	2024-04-08	✗
70	Критическая	CVE-2024-3273	D-Link routers	Сетевой	ACE	2024-04-08	✗
71	Высокая	CVE-2024-31851	CData Products	Сетевой	RLF	2024-04-08	✓
72	Высокая	CVE-2024-31850	CData Products	Сетевой	RLF	2024-04-08	✓

73	Критическая	CVE-2024-31849	CData Products	Сетевой	PE	2024-04-08	✓
74	Критическая	CVE-2024-31848	CData Products	Сетевой	PE	2024-04-08	✓
75	Критическая	None	sngrep	Сетевой	ACE	2024-04-08	✓

1

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2024-2757

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

Уязвимый продукт: PHP: 8.3.0 - 8.3.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://www.php.net/ChangeLog-8.php

2

Краткое описание: Обход безопасности в PHP

Идентификатор уязвимости: CVE-2024-3096

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: PHP: 8.0.0 - 8.3.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://www.php.net/ChangeLog-8.php

3

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: cve-2024-20314

Идентификатор программной ошибки: CWE-783 Уязвимость, связанная с приоритетом операторов

Уязвимый продукт: Cisco IOS XE

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-02632

4

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: cve-2024-20311

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: Cisco IOS XE

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-02636

5

Краткое описание: Обход безопасности в Ruijie RG-NBR700GW

Идентификатор уязвимости: cve-2024-28288

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Ruijie RG-NBR700GW: до версии 10.3(4b12).

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2024-03-30 / 2024-04-01

Ссылки на источник:

6

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-26275

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: 35.1 - 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-222019.html

7

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-35982

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

Уязвимый продукт: SCALANCE W1750D (USA): до 8.10.0.9
SCALANCE W1750D (ROW): до 8.10.0.9
SCALANCE W1750D (JP): до 8.10.0.9

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-885980.txt

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3515

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.107

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_10.html
- http://crbug.com/331123811

9

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-35981

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

Уязвимый продукт: SCALANCE W1750D (USA): до 8.10.0.9
SCALANCE W1750D (ROW): до 8.10.0.9
SCALANCE W1750D (JP): до 8.10.0.9

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-885980.txt

10

Краткое описание: Выполнение произвольного кода в Siemens Scalance W1750D

Идентификатор уязвимости: CVE-2023-35980

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

Уязвимый продукт: SCALANCE W1750D (USA): до 8.10.0.9
SCALANCE W1750D (ROW): до 8.10.0.9
SCALANCE W1750D (JP): до 8.10.0.9

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-11 / 2024-04-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-885980.txt

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3516

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.107

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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_10.html
- http://crbug.com/328859176

12

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-3157

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 123.0.6312.107

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_10.html
- http://crbug.com/331237485

13

Краткое описание: Межсайтовый скриптинг в Microsoft Outlook for Windows

Идентификатор уязвимости: CVE-2024-20670

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Outlook for Windows: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670

Краткое описание: Выполнение произвольного кода в Microsoft WDAC SQL Server ODBC Driver

Идентификатор уязвимости: CVE-2024-26214

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносной базе данных SQL.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26214

Краткое описание: Выполнение произвольного кода в Microsoft Windows libarchive

Идентификатор уязвимости: CVE-2024-26256

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

Уязвимый продукт: Windows: 11 22H2 - 11 23H2
Windows Server: 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

15

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

Оценка CVSSv3: 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: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256

Краткое описание: Выполнение произвольного кода в Microsoft Windows proxy driver

Идентификатор уязвимости: CVE-2024-26234

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

16

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2024-26257

Идентификатор программной ошибки: CWE-415 Двойное освобождение

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

17

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

Оценка CVSSv3: 7.8 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: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

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

Идентификатор уязвимости: CVE-2024-29990

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Azure Kubernetes Service Confidential Containers: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29990

Краткое описание: Выполнение произвольного кода в Rust

Идентификатор уязвимости: CVE-2024-24576

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

Уязвимый продукт: Rust Programming Language: 1.0.0 - 1.77.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Выполнение специально созданного вредоносного файла

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://github.com/rust-lang/rust/security/advisories/GHSA-q455-m56c-85mh
- http://github.com/rust-lang/rust/releases/tag/1.77.2

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

Идентификатор уязвимости: CVE-2024-26210

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

20

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26210

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

Идентификатор уязвимости: CVE-2024-26244

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

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26244

Краткое описание: Получение конфиденциальной информации в Microsoft Windows Cryptographic Services

Идентификатор уязвимости: CVE-2024-26228

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

22

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26228

Краткое описание: Выполнение произвольного кода в Microsoft Windows Cryptographic Services

Идентификатор уязвимости: CVE-2024-29050

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-10 / 2024-04-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29050

Краткое описание: Обход безопасности в Microsoft Windows

Идентификатор уязвимости: CVE-2024-29988

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Обход безопасности

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

24

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
- http://www.zerodayinitiative.com/blog/2024/4/9/the-april-2024-security-updates-review
- http://www.zerodayinitiative.com/advisories/ZDI-24-361/
- https://bdu.fstec.ru/vul/2024-02831

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

Идентификатор уязвимости: CVE-2024-28938

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

25

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28938

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

Идентификатор уязвимости: CVE-2024-28941

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

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

26 **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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28941

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

Идентификатор уязвимости: CVE-2024-29043

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

27 **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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29043

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

Идентификатор уязвимости: CVE-2024-28935

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

28

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28935

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

Идентификатор уязвимости: CVE-2024-28936

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

29

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28936

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

Идентификатор уязвимости: CVE-2024-28931

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

30

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28931

31

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

Идентификатор уязвимости: CVE-2024-28929

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28929

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

Идентификатор уязвимости: CVE-2024-28937

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

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
Visual Studio: 16.0 - 2022 version 17.9
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

32

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28937

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

Идентификатор уязвимости: CVE-2024-28943

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

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

33 **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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28943

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

Идентификатор уязвимости: CVE-2024-28932

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

34

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28932

35

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

Идентификатор уязвимости: CVE-2024-28930

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28930

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

Идентификатор уязвимости: CVE-2024-28933

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 CU12
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

36

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28933

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

Идентификатор уязвимости: CVE-2024-28934

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.9
Microsoft SQL Server: 2019 CU25 - 2022 GDR
Microsoft ODBC Driver for SQL Server on Linux: 17 - 18.0
Microsoft ODBC Driver for SQL Server on macOS: 17 - 18.0
Microsoft ODBC Driver for SQL Server on Windows: 17.0 - 18.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Переполнение буфера

37

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28934

38

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

Идентификатор уязвимости: CVE-2024-20759

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.3.7 - 2.4.7-beta2
Magento Open Source: 2.4.4 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-18.html

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

Идентификатор уязвимости: CVE-2024-20758

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.3.7 - 2.4.7-beta2
Magento Open Source: 2.4.4 - 2.4.7-beta2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

39

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

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-18.html

40

Краткое описание: Выполнение произвольного кода в Adobe Media Encoder

Идентификатор уязвимости: CVE-2024-20772

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

Уязвимый продукт: Adobe Media Encoder: 22.0 - 24.3

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/media-encoder/apsb24-23.html

41

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2024-20795

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

Уязвимый продукт: Animate: 20.0 - 24.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/animate/apsb24-26.html

Краткое описание: Чтение локальных файлов в Adobe Animate

Идентификатор уязвимости: CVE-2024-20797

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Animate: 20.0 - 24.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv3: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://helpx.adobe.com/security/products/animate/apsb24-26.html

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

Идентификатор уязвимости: CVE-2024-29044

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU20 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

43

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29044

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

Идентификатор уязвимости: CVE-2024-28913

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28913

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

Идентификатор уязвимости: CVE-2024-28915

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

45

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28915

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

Идентификатор уязвимости: CVE-2024-28912

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

46

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28912

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

Идентификатор уязвимости: CVE-2024-28909

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

47

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28909

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

Идентификатор уязвимости: CVE-2024-28944

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

48

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28944

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

Идентификатор уязвимости: CVE-2024-29982

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

49

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29982

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

Идентификатор уязвимости: CVE-2024-28914

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

50

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28914

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

Идентификатор уязвимости: CVE-2024-28939

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

51

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28939

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

Идентификатор уязвимости: CVE-2024-28908

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

52

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28908

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

Идентификатор уязвимости: CVE-2024-28926

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

53

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28926

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

Идентификатор уязвимости: CVE-2024-28906

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

54

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28906

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

Идентификатор уязвимости: CVE-2024-29984

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

55

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29984

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

Идентификатор уязвимости: CVE-2024-28911

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

56

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28911

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

Идентификатор уязвимости: CVE-2024-29045

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

57

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

Оценка CVSSv3: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29045

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

Идентификатор уязвимости: CVE-2024-28927

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

58

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28927

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

Идентификатор уязвимости: CVE-2024-28910

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

59

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28910

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

Идентификатор уязвимости: CVE-2024-29046

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

60

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29046

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

Идентификатор уязвимости: CVE-2024-29048

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

61

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29048

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

Идентификатор уязвимости: CVE-2024-28942

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28942

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

Идентификатор уязвимости: CVE-2024-28945

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

63

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28945

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

Идентификатор уязвимости: CVE-2024-29985

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

64

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29985

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

Идентификатор уязвимости: CVE-2024-29983

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft 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: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29983

66

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

Идентификатор уязвимости: CVE-2024-29047

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU25 - 2022 CU12

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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29047

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

Идентификатор уязвимости: CVE-2024-28940

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: 2019 CU20 - 2022 GDR
OLE DB Driver: 18.0.0 - 19.0.0

Категория уязвимого продукта: Операционные системы Microsoft 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: 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: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-28940

Краткое описание: Выполнение произвольного кода в FortiClient for Linux

Идентификатор уязвимости: CVE-2023-45590

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

Уязвимый продукт: FortiClient (Linux): 7.0.0 - 7.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-04-09 / 2024-04-09

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-087

Краткое описание: Выполнение произвольного кода в D-Link routers

Идентификатор уязвимости: CVE-2024-3272

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

Уязвимый продукт: D-Link DNS-320L: все версии
D-Link DNS-325: все версии
D-Link DNS-327L: все версии
D-Link DNS-340L: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

69 **Последствия эксплуатации:** Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://vuldb.com/?id.259283
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

Краткое описание: Выполнение произвольного кода в D-Link routers

Идентификатор уязвимости: CVE-2024-3273

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

Уязвимый продукт: D-Link DNS-320L: все версии
D-Link DNS-325: все версии
D-Link DNS-327L: все версии
D-Link DNS-340L: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

70 **Последствия эксплуатации:** Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://vuldb.com/?id.259284
- http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383
- https://bdu.fstec.ru/vul/2024-02740

Краткое описание: Чтение локальных файлов в CData Products

Идентификатор уязвимости: CVE-2024-31851

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

Уязвимый продукт: CData Sync: до 23.4.8843

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-09

Краткое описание: Чтение локальных файлов в CData Products

Идентификатор уязвимости: CVE-2024-31850

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

Уязвимый продукт: CData Arc: до 23.4.8839

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-09

Краткое описание: Повышение привилегий в CData Products

Идентификатор уязвимости: CVE-2024-31849

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

Уязвимый продукт: CData Connect: до 23.4.8846

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Повышение привилегий

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: 9.8 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: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-09

Краткое описание: Повышение привилегий в CData Products

Идентификатор уязвимости: CVE-2024-31848

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

Уязвимый продукт: CData API Server: до 23.4.8844

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Повышение привилегий

74 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-09

Краткое описание: Выполнение произвольного кода в sngrep

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: sngrep: 1.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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: 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: 2024-04-08 / 2024-04-08

Ссылки на источник:

- http://github.com/irontec/sngrep/releases/tag/v1.8.1