НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-11.1 | 11 октября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-36436	Windows	Локальный	ACE	2023-10-10	✓
2	Высокая	CVE-2023-36710	Windows	Локальный	ACE	2023-10-11	✓
3	Высокая	CVE-2023-36557	Windows Server	Локальный	ACE	2023-10-11	✓
4	Высокая	CVE-2023-36577	Windows	Сетевой	ACE	2023-10-11	✓
5	Высокая	CVE-2023-36418	Azure RTOS GUIX Studio	Локальный	ACE	2023-10-11	✓
6	Высокая	CVE-2023-36725	Windows	Локальный	PE	2023-10-11	✓
7	Средняя	CVE-2023-36576	Windows	Локальный	OSI	2023-10-11	✓
8	Высокая	CVE-2023-36712	Windows	Локальный	PE	2023-10-11	✓
9	Средняя	CVE-2023-36564	Windows	Сетевой	ACE	2023-10-11	✓
10	Высокая	CVE-2023-44487	Jetty	Сетевой	DoS	2023-10-11	✓
11	Высокая	CVE-2023-36598	Microsoft WDAC ODBC Driver	Локальный	ACE	2023-10-10	✓
12	Высокая	CVE-2023-36417	Microsoft SQL Server	Локальный	ACE	2023-10-10	✓
13	Высокая	CVE-2023-36730	Microsoft SQL Server	Локальный	ACE	2023-10-10	✓

14	Высокая	CVE-2023-36785	Microsoft SQL Server	Локальный	ACE	2023-10-10	✓
15	Высокая	CVE-2023-36704	Microsoft Windows Setup Files Cleanup	Локальный	ACE	2023-10-10	✓
16	Высокая	CVE-2023-26370	Adobe Photoshop	Локальный	ACE	2023-10-10	✓
17	Высокая	CVE-2023-41767	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
18	Высокая	CVE-2023-41770	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
19	Высокая	CVE-2023-38166	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
20	Высокая	CVE-2023-41774	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
21	Высокая	CVE-2023-41773	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
22	Высокая	CVE-2023-41769	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
23	Высокая	CVE-2023-41771	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
24	Высокая	CVE-2023-41768	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
25	Высокая	CVE-2023-41765	Microsoft Windows L2TP	Сетевой	ACE	2023-10-10	✓
26	Не определено	CVE-2023-44487	HTTP/2 in Microsoft IIS, Microsoft Visual Studio, Microsoft ASP.NET Core, Microsoft .Net	Не определено	DoS	2023-10-10	✓
27	Критическая	CVE-2023-35349	Microsoft Message Queuing	Сетевой	ACE	2023-10-10	✓
28	Высокая	CVE-2023-36593	Microsoft Message Queuing	Локальный	ACE	2023-10-10	✓

29	Высокая	CVE-2023-36431	Microsoft Message Queuing	Сетевой	DoS	2023-10-10	✓
30	Высокая	CVE-2023-36581	Microsoft Message Queuing	Сетевой	DoS	2023-10-10	✓
31	Высокая	CVE-2023-36579	Microsoft Message Queuing	Сетевой	DoS	2023-10-10	✓
32	Средняя	CVE-2023-3169	WordPress плагин tagDiv Composer	Сетевой	XSS\CSS	2023-09-11	✓
33	Высокая	CVE-2023-40047	WS_FTP Server	Сетевой	ACE	2023-09-29	✓
34	Высокая	CVE-2023-40046	WS_FTP Server	Сетевой	ACE	2023-09-29	✓
35	Высокая	CVE-2023-40045	WS_FTP Server	Сетевой	ACE	2023-09-29	✓
36	Критическая	CVE-2023-42657	WS_FTP Server	Сетевой	OSI	2023-09-29	✓
37	Критическая	CVE-2023-40044	WS_FTP Server	Сетевой	ACE	2023-09-29	✓

1

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-36436

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36436

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-36710

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 R2 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

2

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36710

3

Краткое описание: Выполнение произвольного кода в Windows Server

Идентификатор уязвимости: CVE-2023-36557

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows Server: 2016 - 2022 20H2
Windows: 10 - 11 22H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36557

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-36577

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

4

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36577

Краткое описание: Выполнение произвольного кода в Azure RTOS GUIX Studio

Идентификатор уязвимости: CVE-2023-36418

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Azure RTOS GUIX Studio: до 6.3.0
Azure RTOS GUIX Studio Installer Application: до 6.3.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

5

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36418

6

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2023-36725

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

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2019 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36725

Краткое описание: Получение конфиденциальной информации в Windows

Идентификатор уязвимости: CVE-2023-36576

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

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2016 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

7

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

Оценка CVSSv3: 5.5 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36576

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2023-36712

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

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: повышение привилегий

8

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36712

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-36564

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36564

10

Краткое описание: Отказ в обслуживании в Jetty

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Jetty: 9.0.0.v20130308 - 12.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-11 / 2023-10-11

Ссылки на источник:

- http://github.com/eclipse/jetty.project/issues/10679
- http://github.com/eclipse/jetty.project/releases/tag/jetty-12.0.2
- http://github.com/eclipse/jetty.project/releases/tag/jetty-11.0.17
- http://github.com/eclipse/jetty.project/releases/tag/jetty-10.0.17
- http://github.com/eclipse/jetty.project/releases/tag/jetty-9.4.53.v20231009
- https://bdu.fstec.ru/vul/2023-06559

11

Краткое описание: Выполнение произвольного кода в Microsoft WDAC ODBC Driver

Идентификатор уязвимости: CVE-2023-36598

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft WDAC ODBC Driver:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36598

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2023-36417

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: до 2022 GDR 16.0.1105.1
OLE DB Driver: до 19.3.0002.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36417

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2023-36730

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: до 2022 GDR 16.0.1105.1
Microsoft ODBC Driver for SQL Server on Linux: до 18.3.2.1
Microsoft ODBC Driver for SQL Server on macOS: до 18.3.2.1
Microsoft ODBC Driver for SQL Server on Windows: до 18.6.0007.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

13 **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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36730

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2023-36785

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SQL Server: до 2022 GDR 16.0.1105.1
Microsoft ODBC Driver for SQL Server on Linux: до 18.3.2.1
Microsoft ODBC Driver for SQL Server on macOS: до 18.3.2.1
Microsoft ODBC Driver for SQL Server on Windows: до 18.6.0007.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

14 **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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36785

15

Краткое описание: Выполнение произвольного кода в Microsoft Windows Setup Files Cleanup

Идентификатор уязвимости: CVE-2023-36704

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Setup Files Cleanup:
Windows: 10 - 11 22H2
Windows Server: 2019 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36704

16

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2023-26370

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Adobe Photoshop: 23.0 - 24.7

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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb23-51.html

17

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41767

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41767

18

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41770

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41770

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-38166

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-38166

20

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41774

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41774

21

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41773

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41773

22

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41769

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41769

23

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41771

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41771

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41768

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

24

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

Оценка CVSSv3: 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41768

Краткое описание: Выполнение произвольного кода в Microsoft Windows L2TP

Идентификатор уязвимости: CVE-2023-41765

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Windows L2TP:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 8.1 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: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-41765

Краткое описание: Отказ в обслуживании в HTTP/2 in Microsoft IIS, Microsoft Visual Studio, Microsoft ASP.NET Core, Microsoft .Net

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: HTTP/2 in Microsoft IIS, Microsoft Visual Studio, Microsoft ASP.NET Core, Microsoft .Net:
Windows: 10 - 11 22H2
Windows Server: 2016 - 2022 20H2
Microsoft IIS: 10.0
Visual Studio: 17.2.0 17.2.32505.173 - 17.7.4 17.7.34031.279
ASP.NET Core: before 7.0.12
.NET: 6.0.0 - 7.0.11

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

26 **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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-44487

27

Краткое описание: Выполнение произвольного кода в Microsoft Message Queuing

Идентификатор уязвимости: CVE-2023-35349

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Message Queuing:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-35349

28

Краткое описание: Выполнение произвольного кода в Microsoft Message Queuing

Идентификатор уязвимости: CVE-2023-36593

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Message Queuing:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36593

29

Краткое описание: Отказ в обслуживании в Microsoft Message Queuing

Идентификатор уязвимости: CVE-2023-36431

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Message Queuing:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36431

30

Краткое описание: Отказ в обслуживании в Microsoft Message Queuing

Идентификатор уязвимости: CVE-2023-36581

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Message Queuing:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36581

31

Краткое описание: Отказ в обслуживании в Microsoft Message Queuing

Идентификатор уязвимости: CVE-2023-36579

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Message Queuing:
Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36579

Краткое описание: Межсайтовый скриптинг в WordPress плагин tagDiv Composer

Идентификатор уязвимости: CVE-2023-3169

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

Уязвимый продукт: WordPress плагин tagDiv Composer: до версии 4.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: межсайтовый скриптинг

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-11 / 2023-09-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-3169

Краткое описание: Выполнение произвольного кода в WS_FTP Server

Идентификатор уязвимости: CVE-2023-40047

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

Уязвимый продукт: WS_FTP Server: 8.8.0 - 8.8.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-29 / 2023-09-29

Ссылки на источник:

- http://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023

Краткое описание: Выполнение произвольного кода в WS_FTP Server

Идентификатор уязвимости: CVE-2023-40046

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

Уязвимый продукт: WS_FTP Server: 8.0.0 - 8.8.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-29 / 2023-09-29

Ссылки на источник:

- http://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023

Краткое описание: Выполнение произвольного кода в WS_FTP Server

Идентификатор уязвимости: CVE-2023-40045

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

Уязвимый продукт: WS_FTP Server: 8.0.0 - 8.8.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-29 / 2023-09-29

Ссылки на источник:

- http://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023

Краткое описание: Получение конфиденциальной информации в WS_FTP Server

Идентификатор уязвимости: CVE-2023-42657

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

Уязвимый продукт: WS_FTP Server: 7.0 - 8.8.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-29 / 2023-09-29

Ссылки на источник:

- http://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023

37

Краткое описание: Выполнение произвольного кода в WS_FTP Server

Идентификатор уязвимости: CVE-2023-40044

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: WS_FTP Server: 7.0 - 8.8.1

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: 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: 2023-09-29 / 2023-09-29

Ссылки на источник:

- http://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023
- https://bdu.fstec.ru/vul/2023-06356