НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-13.1 | 13 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-36771	Microsoft 3D Builder	Локальный	ACE	2023-09-12	✓
2	Высокая	CVE-2023-36772	Microsoft 3D Builder	Локальный	ACE	2023-09-12	✓
3	Высокая	CVE-2023-36773	Microsoft 3D Builder	Локальный	ACE	2023-09-12	✓
4	Высокая	CVE-2023-36770	Microsoft 3D Builder	Локальный	ACE	2023-09-12	✓
5	Высокая	CVE-2023-38076	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
6	Высокая	CVE-2023-38075	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
7	Высокая	CVE-2023-38074	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
8	Высокая	CVE-2023-36740	Microsoft 3D Viewer	Локальный	ACE	2023-09-12	✓
9	Высокая	CVE-2023-40727	Siemens QMS Automotive	Локальный	ACE	2023-09-13	✓
10	Высокая	CVE-2023-36739	Microsoft 3D Viewer	Локальный	ACE	2023-09-12	✓
11	Высокая	CVE-2023-36760	Microsoft 3D Viewer	Локальный	ACE	2023-09-12	✓
12	Высокая	CVE-2023-38073	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓

13	Высокая	CVE-2023-40726	Siemens QMS Automotive	Сетевой	OSI	2023-09-13	✓
14	Высокая	CVE-2023-38072	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
15	Высокая	CVE-2023-38163	Microsoft Defender Security Intelligence Updates	Локальный	SB	2023-09-13	✓
16	Высокая	CVE-2023-38071	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
17	Высокая	CVE-2023-38070	Siemens Teamcenter Visualization and JT2Go	Локальный	ACE	2023-09-13	✓
18	Высокая	CVE-2023-36742	Visual Studio Code	Локальный	ACE	2023-09-13	✓
19	Высокая	CVE-2023-36788	Microsoft .NET Framework	Локальный	ACE	2023-09-13	✓
20	Высокая	CVE-2023-4909	Google Chrome	Сетевой	OSI	2023-09-13	✓
21	Высокая	CVE-2023-4908	Google Chrome	Сетевой	OSI	2023-09-13	✓
22	Высокая	CVE-2023-4907	Google Chrome	Сетевой	OSI	2023-09-13	✓
23	Высокая	CVE-2023-4906	Google Chrome	Сетевой	OSI	2023-09-13	✓
24	Высокая	CVE-2023-4905	Google Chrome	Сетевой	OSI	2023-09-13	✓
25	Высокая	CVE-2023-4904	Google Chrome	Сетевой	OSI	2023-09-13	✓
26	Высокая	CVE-2023-4903	Google Chrome	Сетевой	OSI	2023-09-13	✓

27	Высокая	CVE-2023-4902	Google Chrome	Сетевой	OSI	2023-09-13	✓
28	Высокая	CVE-2023-4901	Google Chrome	Сетевой	OSI	2023-09-13	✓
29	Высокая	CVE-2023-38146	Microsoft Windows Themes	Сетевой	ACE	2023-09-13	✓
30	Высокая	CVE-2023-4900	Google Chrome	Сетевой	OSI	2023-09-13	✓
31	Высокая	CVE-2023-36794	Microsoft Visual Studio	Локальный	ACE	2023-09-12	✓
32	Высокая	CVE-2023-36793	Microsoft Visual Studio	Локальный	ACE	2023-09-12	✓
33	Высокая	CVE-2023-36792	Microsoft Visual Studio	Локальный	ACE	2023-09-12	✓
34	Высокая	CVE-2023-36758	Microsoft Visual Studio	Локальный	PE	2023-09-12	✓
35	Высокая	CVE-2023-36796	Microsoft Visual Studio	Локальный	ACE	2023-09-12	✓
36	Средняя	CVE-2023-36761	Microsoft Office	Локальный	OSI	2023-09-12	✓
37	Высокая	CVE-2023-4863	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2023-09-12	✓
38	Средняя	CVE-2023-36761	Microsoft Office	Локальный	OSI	2023-09-12	✓
39	Высокая	CVE-2023-29332	Microsoft Azure Kubernetes Service	Сетевой	PE	2023-09-12	✓
40	Высокая	CVE-2023-41033	Siemens Parasolid	Локальный	ACE	2023-09-12	✓
41	Высокая	CVE-2023-41032	Siemens Parasolid	Локальный	ACE	2023-09-12	✓

42	Высокая	CVE-2023-26369	Adobe Acrobat and Reader	Локальный	ACE	2023-09-12	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft 3D Builder

Идентификатор уязвимости: CVE-2023-36771

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Builder: до 20.0.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36771

2

Краткое описание: Выполнение произвольного кода в Microsoft 3D Builder

Идентификатор уязвимости: CVE-2023-36772

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Builder: до 20.0.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36772

3

Краткое описание: Выполнение произвольного кода в Microsoft 3D Builder

Идентификатор уязвимости: CVE-2023-36773

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Builder: до 20.0.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36773

4

Краткое описание: Выполнение произвольного кода в Microsoft 3D Builder

Идентификатор уязвимости: CVE-2023-36770

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Builder: до 20.0.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36770

5

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

Идентификатор уязвимости: CVE-2023-38076

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

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

6

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

Идентификатор уязвимости: CVE-2023-38075

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

7

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

Идентификатор уязвимости: CVE-2023-38074

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

8

Краткое описание: Выполнение произвольного кода в Microsoft 3D Viewer

Идентификатор уязвимости: CVE-2023-36740

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Viewer: до 7.2306.12012.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36740

Краткое описание: Выполнение произвольного кода в Siemens QMS Automotive

Идентификатор уязвимости: CVE-2023-40727

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Siemens QMS Automotive: до 12.39

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-147266.pdf

Краткое описание: Выполнение произвольного кода в Microsoft 3D Viewer

Идентификатор уязвимости: CVE-2023-36739

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Viewer: до 7.2306.12012.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36739

11

Краткое описание: Выполнение произвольного кода в Microsoft 3D Viewer

Идентификатор уязвимости: CVE-2023-36760

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 3D Viewer: до 7.2306.12012.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36760

12

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

Идентификатор уязвимости: CVE-2023-38073

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

13

Краткое описание: Получение конфиденциальной информации в Siemens QMS Automotive

Идентификатор уязвимости: CVE-2023-40726

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

Уязвимый продукт: Siemens QMS Automotive: до 12.39

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-147266.pdf

14

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

Идентификатор уязвимости: CVE-2023-38072

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

Краткое описание: Обход безопасности в Microsoft Defender Security Intelligence Updates

Идентификатор уязвимости: CVE-2023-38163

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Defender Security Intelligence Updates: до 1.391.1332.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-38163

16

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

Идентификатор уязвимости: CVE-2023-38071

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

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

17

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

Идентификатор уязвимости: CVE-2023-38070

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Siemens Teamcenter Visualization and JT2Go:
JT2Go: до 14.3.0.1
Teamcenter Visualization: 13.3 - 14.3

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-278349.pdf

18

Краткое описание: Выполнение произвольного кода в Visual Studio Code

Идентификатор уязвимости: CVE-2023-36742

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Visual Studio Code: 1.0.0 - 1.82.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36742
- http://github.com/microsoft/vscode/security/advisories/GHSA-r6q2-478f-5gmr

Краткое описание: Выполнение произвольного кода в Microsoft .NET Framework

Идентификатор уязвимости: CVE-2023-36788

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft .NET Framework: до 4.8.09186.01

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36788

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4909

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1463293

21

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4908

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1451543

22

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4907

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1462104

23

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4906

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1449874

24

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4905

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1441228

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4904

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1453501

26

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4903

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1446709

27

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4902

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1454515

28

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4901

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1459281

Краткое описание: Выполнение произвольного кода в Microsoft Windows Themes

Идентификатор уязвимости: CVE-2023-38146

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Themes:
Windows: 10 - 11 22H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

29

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-38146

30

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4900

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 116.0.5845.188

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-13 / 2023-09-13

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
- http://crbug.com/1430867

31

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2023-36794

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Visual Studio: 16.0 - 2022 version 17.7
Microsoft .NET Framework: 2.0 Service Pack 2 - 4.8.1
.NET: 6.0.0 - 7.0.0

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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36794

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2023-36793

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Visual Studio: 16.0 - 2022 version 17.7
Microsoft .NET Framework: 2.0 Service Pack 2 - 4.8.1
.NET: 6.0.0 - 7.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

32

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

Оценка CVSSv3: 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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36793

33

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2023-36792

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Visual Studio: до 17.7.4 17.7.34031.279
Microsoft .NET Framework: до 4.8.09186.01
.NET: до 7.0.11

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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36792

Краткое описание: Повышение привилегий в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2023-36758

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

Уязвимый продукт: Microsoft Visual Studio: до 17.7.4 17.7.34031.279

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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: 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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36758

35

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2023-36796

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Visual Studio: 16.0 - 2022 version 17.7
Microsoft .NET Framework: 2.0 Service Pack 2 - 4.8.1
.NET: 6.0.0 - 7.0.0

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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36796

36

Краткое описание: Получение конфиденциальной информации в Microsoft Office

Идентификатор уязвимости: CVE-2023-36761

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

Уязвимый продукт: Microsoft Office: 365 - 2019
Microsoft Word: до 16.0.5413.1000
Microsoft 365 Apps for Enterprise: до 16.0.5413.1000

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 6.2 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36761

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2023-4863

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

Уязвимый продукт: Mozilla Firefox and Firefox ESR:
Firefox for Android: 66.0.4 - 117.0
Firefox for iOS: 8.0 - 117.0
Mozilla Firefox: 100.0 - 117.0
Firefox ESR: 102.0 - 115.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2023-40/

38

Краткое описание: Получение конфиденциальной информации в Microsoft Office

Идентификатор уязвимости: CVE-2023-36761

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

Уязвимый продукт: Microsoft Office: 365 - 2019
Microsoft Word: до 16.0.5413.1000
Microsoft 365 Apps for Enterprise: до 16.0.5413.1000

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 6.2 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36761

Краткое описание: Повышение привилегий в Microsoft Azure Kubernetes Service

Идентификатор уязвимости: CVE-2023-29332

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

Уязвимый продукт: Microsoft Azure Kubernetes Service: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29332

Краткое описание: Выполнение произвольного кода в Siemens Parasolid

Идентификатор уязвимости: CVE-2023-41033

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens Parasolid: 35.0 - 36.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-190839.pdf

41

Краткое описание: Выполнение произвольного кода в Siemens Parasolid

Идентификатор уязвимости: CVE-2023-41032

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens Parasolid: 34.1 - 36.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-190839.pdf

42

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2023-26369

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat and Reader:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 23.003.20284

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: 2023-09-12 / 2023-09-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-34.html