НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-14.1 | 14 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-24489	Citrix ShareFile storage zones controller	Сетевой	SB	2023-07-13	✓
2	Высокая	CVE-2023-28730	Panasonic Control FPWIN	Локальный	ACE	2023-07-13	✓
3	Высокая	CVE-2023-28729	Panasonic Control FPWIN	Локальный	ACE	2023-07-13	✓
4	Высокая	CVE-2023-28728	Panasonic Control FPWIN	Локальный	ACE	2023-07-13	✓
5	Высокая	CVE-2023-0215	Siemens SIMATIC MV500 Devices	Сетевой	DoS	2023-07-13	✓
6	Высокая	CVE-2023-35920	Siemens SIMATIC MV500 Devices	Сетевой	DoS	2023-07-13	✓
7	Высокая	CVE-2023-35921	Siemens SIMATIC MV500 Devices	Сетевой	DoS	2023-07-13	✓
8	Высокая	CVE-2023-36521	Siemens SIMATIC MV500 Devices	Сетевой	DoS	2023-07-13	✓
9	Высокая	CVE-2023-37376	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓
10	Высокая	CVE-2023-37375	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓
11	Высокая	CVE-2023-37374	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓
12	Высокая	CVE-2023-37248	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓
13	Высокая	CVE-2023-37247	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓

14	Высокая	CVE-2023-37246	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2023-07-13	✓
15	Критическая	CVE-2023-20214	Cisco SD-WAN vManage	Сетевой	SB	2023-07-13	✓
16	Высокая	CVE-2023-33170	Microsoft ASP.NET and Visual Studio	Сетевой	PE	2023-07-12	✓
17	Высокая	CVE-2023-35313	Microsoft Windows Online Certificate Status Protocol (OCSP) SnapIn	Локальный	ACE	2023-07-12	✓
18	Высокая	CVE-2023-32038	Microsoft ODBC Driver	Сетевой	ACE	2023-07-12	✓
19	Высокая	CVE-2023-36867	Visual Studio Code - GitHub Pull Requests and Issues Extension	Локальный	ACE	2023-07-12	✓
20	Высокая	CVE-2023-36867	Microsoft Visual Studio Code GitHub Pull Requests and Issues Extension	Локальный	ACE	2023-07-12	✓
21	Высокая	CVE-2023-33152	Microsoft ActiveX	Локальный	ACE	2023-07-12	✓
22	Высокая	CVE-2023-35343	Microsoft Windows Geolocation Service	Локальный	ACE	2023-07-12	✓
23	Высокая	CVE-2023-33161	Microsoft Excel	Локальный	ACE	2023-07-12	✓
24	Высокая	CVE-2023-33158	Microsoft Excel	Локальный	ACE	2023-07-12	✓
25	Критическая	CVE-2023-35365	Microsoft Windows Routing and Remote Access Service	Сетевой	ACE	2023-07-12	✓
26	Критическая	CVE-2023-35366	Microsoft Windows Routing and Remote Access Service	Сетевой	ACE	2023-07-12	✓
27	Критическая	CVE-2023-35367	Microsoft Windows Routing and Remote Access Service	Сетевой	ACE	2023-07-12	✓

28	Высокая	CVE-2023-35323	Microsoft Windows OLE	Локальный	ACE	2023-07-12	✓

1

Краткое описание: Обход безопасности в Citrix ShareFile storage zones controller

Идентификатор уязвимости: CVE-2023-24489

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Citrix ShareFile storage zones controller: до 5.11.24

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://support.citrix.com/article/CTX559517/sharefile-storagezones-controller-security-update-for-cve202324489
- https://bdu.fstec.ru/vul/2023-03161

2

Краткое описание: Выполнение произвольного кода в Panasonic Control FPWIN

Идентификатор уязвимости: CVE-2023-28730

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

Уязвимый продукт: Panasonic Control FPWIN: 7.6.0.3 - 7.6.0.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-192-03

3

Краткое описание: Выполнение произвольного кода в Panasonic Control FPWIN

Идентификатор уязвимости: CVE-2023-28729

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

Уязвимый продукт: Panasonic Control FPWIN: 7.6.0.3 - 7.6.0.3

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-192-03

4

Краткое описание: Выполнение произвольного кода в Panasonic Control FPWIN

Идентификатор уязвимости: CVE-2023-28728

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Panasonic Control FPWIN: 7.6.0.3 - 7.6.0.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-192-03

Краткое описание: Отказ в обслуживании в Siemens SIMATIC MV500 Devices

Идентификатор уязвимости: CVE-2023-0215

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Siemens SIMATIC MV500 Devices:
SIMATIC MV560 X: до 3.3.4
SIMATIC MV560 U: до 3.3.4
SIMATIC MV550 S: до 3.3.4
SIMATIC MV550 H: до 3.3.4
SIMATIC MV540 S: до 3.3.4
SIMATIC MV540 H: до 3.3.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

5 **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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-561322.txt
- https://bdu.fstec.ru/vul/2023-00675

6

Краткое описание: Отказ в обслуживании в Siemens SIMATIC MV500 Devices

Идентификатор уязвимости: CVE-2023-35920

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

Уязвимый продукт: Siemens SIMATIC MV500 Devices:
SIMATIC MV560 X: до 3.3.4
SIMATIC MV560 U: до 3.3.4
SIMATIC MV550 S: до 3.3.4
SIMATIC MV550 H: до 3.3.4
SIMATIC MV540 S: до 3.3.4
SIMATIC MV540 H: до 3.3.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-561322.txt

7

Краткое описание: Отказ в обслуживании в Siemens SIMATIC MV500 Devices

Идентификатор уязвимости: CVE-2023-35921

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

Уязвимый продукт: Siemens SIMATIC MV500 Devices:
SIMATIC MV560 X: до 3.3.4
SIMATIC MV560 U: до 3.3.4
SIMATIC MV550 S: до 3.3.4
SIMATIC MV550 H: до 3.3.4
SIMATIC MV540 S: до 3.3.4
SIMATIC MV540 H: до 3.3.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-561322.txt

8

Краткое описание: Отказ в обслуживании в Siemens SIMATIC MV500 Devices

Идентификатор уязвимости: CVE-2023-36521

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Siemens SIMATIC MV500 Devices:
SIMATIC MV560 X: до 3.3.4
SIMATIC MV560 U: до 3.3.4
SIMATIC MV550 S: до 3.3.4
SIMATIC MV550 H: до 3.3.4
SIMATIC MV540 S: до 3.3.4
SIMATIC MV540 H: до 3.3.4

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-561322.txt

9

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37376

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37375

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37374

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

11 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37248

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37247

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

13 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2023-37246

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

Уязвимый продукт: Siemens Tecnomatix Plant Simulation: 2201 - 2302

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

Краткое описание: Обход безопасности в Cisco SD-WAN vManage

Идентификатор уязвимости: CVE-2023-20214

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Cisco SD-WAN vManage: 20.6.3.3 - 20.11

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-13 / 2023-07-13

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA

16

Краткое описание: Повышение привилегий в Microsoft ASP.NET and Visual Studio

Идентификатор уязвимости: CVE-2023-33170

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Microsoft ASP.NET and Visual Studio:
ASP.NET 6.0.0 - 7.0.0
Visual Studio 2022 version 17.0 - 2022 version 17.6

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33170

Краткое описание: Выполнение произвольного кода в Microsoft Windows Online Certificate Status Protocol (OCSP) SnapIn

Идентификатор уязвимости: CVE-2023-35313

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Online Certificate Status Protocol (OCSP) SnapIn:
Windows 10 - 11 22H2
Windows Server 2016 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313

Краткое описание: Выполнение произвольного кода в Microsoft ODBC Driver

Идентификатор уязвимости: CVE-2023-32038

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft 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

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038

Краткое описание: Выполнение произвольного кода в Visual Studio Code - GitHub Pull Requests and Issues Extension

Идентификатор уязвимости: CVE-2023-36867

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Visual Studio Code - GitHub Pull Requests and Issues Extension: все версии

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36867

20

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio Code GitHub Pull Requests and Issues Extension

Идентификатор уязвимости: CVE-2023-36867

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Visual Studio Code GitHub Pull Requests and Issues Extension: все версии

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36867

21

Краткое описание: Выполнение произвольного кода в Microsoft ActiveX

Идентификатор уязвимости: CVE-2023-33152

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft ActiveX:
Microsoft Office 2013 RT Service Pack 1 - 2019
Microsoft Office LTSC 2021 32 bit editions - 64 bit editions
Microsoft 365 Apps for Enterprise 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.0 AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152

Краткое описание: Выполнение произвольного кода в Microsoft Windows Geolocation Service

Идентификатор уязвимости: CVE-2023-35343

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Geolocation Service:
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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343

23

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2023-33161

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Excel:
Microsoft Office 2019 for Mac - 2019 for Mac
Microsoft Office LTSC 2021 2021 for Mac - 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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33161

24

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2023-33158

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Excel:
Microsoft Office 2019 for Mac - 2019 for Mac
Microsoft Office for Universal все версии
Microsoft Office LTSC 2021 32 bit editions - 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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33158

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service

Идентификатор уязвимости: CVE-2023-35365

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Routing and Remote Access Service:
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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35365

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service

Идентификатор уязвимости: CVE-2023-35366

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Routing and Remote Access Service:
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

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35366

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service

Идентификатор уязвимости: CVE-2023-35367

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Routing and Remote Access Service:
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

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35367

Краткое описание: Выполнение произвольного кода в Microsoft Windows OLE

Идентификатор уязвимости: CVE-2023-35323

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows OLE:
Windows Server 2019 - 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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35323