НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-08-10.1 | 10 августа 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-36534	Zoom Desktop Client для Windows	Сетевой	PE	2023-08-08	✓
2	Высокая	CVE-2023-38185	Microsoft Exchange Server 2016 CU23/2019 CU12/2019 CU13	Сетевой	ACE	2023-08-08	✓
3	Высокая	CVE-2023-38212	Adobe Dimension	Локальный	ACE	2023-08-09	✓
4	Высокая	CVE-2023-3867	Linux Kernel	Сетевой	OSI	2023-07-20	✓
5	Высокая	CVE-2023-38125	Softing edgeAggregator	Сетевой	ACE	2023-01-22	✗
6	Высокая	CVE-2023-27336	edgeConnector Siemens	Сетевой	DoS	2023-02-22	✗
7	Высокая	CVE-2022-47185	Apache Traffic Server	Сетевой	DoS	2023-08-09	✓
8	Критическая	CVE-2023-33934	Apache Traffic Server	Сетевой	SB	2023-08-09	✓

Краткое описание: Повышение привилегий в Zoom Desktop Client для Windows

Идентификатор уязвимости: CVE-2023-36534

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

Уязвимый продукт: Zoom Desktop Client для Windows: до 5.14.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.3 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-08-08 / 2023-08-08

Ссылки на источник:

- https://exchange.xforce.ibmcloud.com/vulnerabilities/262825

2

Краткое описание: Выполнение произвольного кода в Microsoft Exchange Server 2016 CU23/2019 CU12/2019 CU13

Идентификатор уязвимости: CVE-2023-38185

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Exchange Server 2016 CU23/2019 CU12/2019 CU13

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-08 / 2023-08-08

Ссылки на источник:

- https://threats.kaspersky.com/ru/vulnerability/KLA51713/

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2023-38212

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

Уязвимый продукт: Adobe Dimension: 3.4.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

3 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2023-08-09 / 2023-08-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/dimension/apsb23-44.html

Краткое описание: Получение конфиденциальной информации в Linux Kernel

Идентификатор уязвимости: CVE-2023-3867

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux Kernel

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-07-20 / 2023-07-28

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-23-981/

5

Краткое описание: Выполнение произвольного кода в Softing edgeAggregator

Идентификатор уязвимости: CVE-2023-38125

Идентификатор программной ошибки: CWE-942 Некорректный междоменный белый список

Уязвимый продукт: Softing edgeAggregator

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-01-22 / 2023-08-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-23-1059/

6

Краткое описание: Отказ в обслуживании в edgeConnector Siemens

Идентификатор уязвимости: CVE-2023-27336

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: edgeConnector Siemens

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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: 2023-02-22 / 2023-08-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-23-1065/

Краткое описание: Отказ в обслуживании в Apache Traffic Server

Идентификатор уязвимости: CVE-2022-47185

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache Traffic Server: 8.1.8, 9.2.2 или позднее

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2023-08-09 / 2023-08-09

Ссылки на источник:

- https://exchange.xforce.ibmcloud.com/vulnerabilities/262956

Краткое описание: Обход безопасности в Apache Traffic Server

Идентификатор уязвимости: CVE-2023-33934

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache Traffic Server: 8.1.8, 9.2.2 или позднее

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

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: 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

Дата выявления / Дата обновления: 2023-08-09 / 2023-08-09

Ссылки на источник:

- https://exchange.xforce.ibmcloud.com/vulnerabilities/262957