НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-03.1 | 3 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-3422	Microsoft Edge	Сетевой	ACE	2023-06-30	✓
2	Высокая	CVE-2023-3421	Microsoft Edge	Сетевой	ACE	2023-06-30	✓
3	Высокая	CVE-2023-3420	Microsoft Edge	Сетевой	ACE	2023-06-30	✓
4	Критическая	CVE-2023-3460	Ultimate Member – User Profile & Membership Plugin	Сетевой	SB	2023-06-30	✓
5	Критическая	CVE-2023-34347	Delta Electronics InfraSuite Device Master	Сетевой	ACE	2023-06-30	✓
6	Высокая	CVE-2023-30765	Delta Electronics InfraSuite Device Master	Сетевой	PE	2023-06-30	✓
7	Критическая	CVE-2023-31222	Medtronic Paceart Optima System	Сетевой	ACE	2023-06-30	✓
8	Высокая	CVE-2023-1049	Schneider Electric EcoStruxure Operator Terminal Expert	Локальный	ACE	2023-06-30	✓
9	Высокая	CVE-2023-24998	Unified Data Protection	Сетевой	DoS	2023-06-29	✓
10	Критическая	CVE-2023-26119	HtmlUnit	Сетевой	ACE	2023-06-28	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-3422

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 114.0.1823.58

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-3422

2

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-3421

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 114.0.1823.58

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-3421

3

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-3420

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 114.0.1823.58

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-3420
- https://bdu.fstec.ru/vul/2023-03442

4

Краткое описание: Обход безопасности в Ultimate Member – User Profile & Membership Plugin

Идентификатор уязвимости: CVE-2023-3460

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Ultimate Member – User Profile & Membership Plugin: 2.6.3 - 2.6.5

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://wordpress.org/support/topic/security-issue-144/#post-16859857
- http://www.bleepingcomputer.com/news/security/hackers-exploit-zero-day-in-ultimate-member-wordpress-plugin-with-200k-installs/

Краткое описание: Выполнение произвольного кода в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-34347

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-180-01

6

Краткое описание: Повышение привилегий в Delta Electronics InfraSuite Device Master

Идентификатор уязвимости: CVE-2023-30765

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Delta Electronics InfraSuite Device Master: до 1.0.7

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.8 AV:N/AC:L/PR:L/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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-180-01

7

Краткое описание: Выполнение произвольного кода в Medtronic Paceart Optima System

Идентификатор уязвимости: CVE-2023-31222

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Medtronic Paceart Optima System: 1.11 - 1.11

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: 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: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://global.medtronic.com/xg-en/product-security/security-bulletins/paceart-optima-system.html
- http://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-180-01

8

Краткое описание: Выполнение произвольного кода в Schneider Electric EcoStruxure Operator Terminal Expert

Идентификатор уязвимости: CVE-2023-1049

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

Уязвимый продукт: Schneider Electric EcoStruxure Operator Terminal Expert: 3.3 SP1 - 3.3 SP1

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-30 / 2023-06-30

Ссылки на источник:

- http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-164-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-164-01.pdf
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-180-02
- https://bdu.fstec.ru/vul/2023-03212

Краткое описание: Отказ в обслуживании в Unified Data Protection

Идентификатор уязвимости: CVE-2023-24998

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

Уязвимый продукт: Unified Data Protection: 7.0 - 9.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 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: 2023-06-29 / 2023-06-29

Ссылки на источник:

- http://documentation.arcserve.com/Arcserve-UDP/Available/9.0/ENU/Bookshelf_Files/HTML/Update1/default.htm#Issues_Fixed.htm?TocPath=____9
- https://bdu.fstec.ru/vul/2023-02037

10

Краткое описание: Выполнение произвольного кода в HtmlUnit

Идентификатор уязвимости: CVE-2023-26119

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

Уязвимый продукт: HtmlUnit: 2.0 - 2.70.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-06-28 / 2023-06-28

Ссылки на источник:

- http://siebene.github.io/2022/12/30/HtmlUnit-RCE/
- http://security.snyk.io/vuln/SNYK-JAVA-NETSOURCEFORGEHTMLUNIT-3252500
- http://github.com/HtmlUnit/htmlunit/commit/641325bbc84702dc9800ec7037aec061ce21956b