НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-10.1 | 10 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-4804	Johnson Controls Quantum HD Unity	Сетевой	CI	2023-11-10	✓
2	Высокая	CVE-2023-5996	Microsoft Edge	Сетевой	ACE	2023-11-10	✓
3	Высокая	CVE-2023-47586	FUJI ELECTRIC products	Локальный	ACE	2023-11-10	✓
4	Высокая	CVE-2023-47585	FUJI ELECTRIC products	Локальный	OSI	2023-11-10	✓
5	Высокая	CVE-2023-47584	FUJI ELECTRIC products	Локальный	ACE	2023-11-10	✓
6	Высокая	CVE-2023-47583	FUJI ELECTRIC products	Локальный	OSI	2023-11-10	✓
7	Высокая	CVE-2023-47582	FUJI ELECTRIC products	Локальный	ACE	2023-11-10	✓
8	Высокая	CVE-2023-47581	FUJI ELECTRIC products	Локальный	OSI	2023-11-10	✓
9	Высокая	CVE-2023-47580	FUJI ELECTRIC products	Локальный	ACE	2023-11-10	✓
10	Не определено	CVE-2023-47246	SysAid	Не определено	ACE	2023-11-09	✓
11	Высокая	CVE-2023-5869	PostgreSQL	Сетевой	ACE	2023-11-09	✓

1

Краткое описание: Внедрение кода в Johnson Controls Quantum HD Unity

Идентификатор уязвимости: CVE-2023-4804

Идентификатор программной ошибки: CWE-489 Присутствует код отладки

Уязвимый продукт: Johnson Controls Quantum HD Unity:
Quantum HD Unity Compressor control panels (Q5): до 11.22
Quantum HD Unity Compressor control panels (Q6): до 12.22
Quantum HD Unity AcuAir control panels(Q5): до 11.12
Quantum HD Unity AcuAir control panels(Q6): до 12.12
Quantum HD Unity Condenser/Vessel control panels (Q5): до 11.11
Quantum HD Unity Condenser/Vessel control panels (Q6): до 12.11
Quantum HD Unity Evaporator control panels (Q5): до 11.11
Quantum HD Unity Evaporator control panels (Q6): до 12.11
Quantum HD Unity Engine Room control panels (Q5): до 11.11
Quantum HD Unity Engine Room control panels (Q6): до 12.11
Quantum HD Unity Interface control panels (Q5): до 11.11
Quantum HD Unity Interface control panels (Q6): до 12.11

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: внедрение кода

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-313-01

- http://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2023/jci-psa-2023-09.pdf?la=en&hash=3A4A98244141122D9019B5EAF3B58314DAA63E4D

2

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2023-5996

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 119.0.2151.44

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

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

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-5996

Краткое описание: Выполнение произвольного кода в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47586

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

Уязвимый продукт: FUJI ELECTRIC products:
V-Sever: 4.0.18.0
V-Sever Lite: 4.0.18.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

4

Краткое описание: Получение конфиденциальной информации в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47585

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FUJI ELECTRIC products:
V-Sever: 4.0.18.0
V-Sever Lite: 4.0.18.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

Краткое описание: Выполнение произвольного кода в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47584

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FUJI ELECTRIC products:
V-Sever: 4.0.18.0
V-Sever Lite: 4.0.18.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

5

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

6

Краткое описание: Получение конфиденциальной информации в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47583

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FUJI ELECTRIC products:
TELLUS Simulator: 4.0.17.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

Краткое описание: Выполнение произвольного кода в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47582

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: FUJI ELECTRIC products:
TELLUS: 4.0.17.0
TELLUS Lite: 4.0.17.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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: 7.8 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: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

8

Краткое описание: Получение конфиденциальной информации в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47581

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FUJI ELECTRIC products:
TELLUS: 4.0.17.0
TELLUS Lite: 4.0.17.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html

Краткое описание: Выполнение произвольного кода в FUJI ELECTRIC products

Идентификатор уязвимости: CVE-2023-47580

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

Уязвимый продукт: FUJI ELECTRIC products:
TELLUS: 4.0.17.0
TELLUS Lite: 4.0.17.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU93840158/index.html
- http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php

10

Краткое описание: Выполнение произвольного кода в SysAid

Идентификатор уязвимости: CVE-2023-47246

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

Уязвимый продукт: SysAid: 21.4.45 - 23.3.35

Категория уязвимого продукта: Прикладное программное обеспечение

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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

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

Ссылки на источник:

- http://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification
- http://twitter.com/msftsecintel/status/1722444141081076219

11

Краткое описание: Выполнение произвольного кода в PostgreSQL

Идентификатор уязвимости: CVE-2023-5869

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: PostgreSQL: 11.0 - 16.0

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: 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: 2023-11-09 / 2023-11-09

Ссылки на источник:

- http://www.postgresql.org/about/news/postgresql-161-155-1410-1313-1217-and-1122-released-2749/