

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230111.9 | 11 января 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Fuji Electric V-Server

| | |
|------------------------------|--|
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимый продукт | V-Server: 4.0.12.0 |
| Дата выявления | 3 января 2023 г. |
| Дата обновления | 3 января 2023 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|--------------------------|---|----------------------|
| MITRE: CVE-2022-47908 | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>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.</p> | 7.8 |

| | | |
|----------------------------------|--|------------|
| <p>MITRE: CVE-2022-41645</p> | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику прочитать содержимое памяти в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничным условием.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-125: Чтение за пределами буфера</p> <p>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.</p> | <p>7.8</p> |
| <p>MITRE: CVE-2022-47317</p> | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-787: Запись за границами буфера</p> <p>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.</p> | <p>7.8</p> |

Ссылки на
источники

http://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php
<http://jvn.jp/en/vu/JVNVU92811888/index.html>