НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230111.8 | 11 января 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Fuji Electric V-SFT and TELLUS

Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Monitouch V-SFT: 6.1.7.0 TELLUS: 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-2022-46360	Эксплуатация уязвимости позволяет локальному злоумышленнику прочитать содержимое памяти в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничным условием. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-125: Чтение за пределами буфера Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации	7.8

	рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	
MITRE: CVE-2022-43448	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-787: Запись за границами буфера 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.	7.8

Ссылки на источники	http://jvn.jp/en/vu/JVNVU90679513/index.html http://monitouch.fujielectric.com/site/download-e/09vsft6_inf/index.php