НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230111.2 | 11 января 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Fuji Electric Tellus Lite V-Simulator

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Tellus Lite V-Simulator: 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-2022-3087	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе. 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

MITRE: CVE-2022-3085	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-121: Переполнение буфера в стеке 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://ics-cert.us-cert.gov/advisories/icsa-22-354-01