НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210722.3 | 22 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в контролере Mitsubishi Electric серии MELSEC-F

Идентификатор уязвимости	MITRE: CVE-2021-20596
Идентификатор программной ошибки	CWE-476: Разыменование нулевого указателя
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена разыменованием нулевого указателя.
Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	MELSEC-F FX3U-ENET: 1.14MELSEC-F FX3U-ENET-L: 1.14MELSEC-F FX3U-ENET-P502: 1.14
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 июля 2021 г.
Дата обновления	21 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021072103 https://ics-cert.us-cert.gov/advisories/icsa-21-201-01