НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200414.1 | 14 апреля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Fuji Electric V-Server Lite

Идентификатор уязвимости	MITRE: CVE-2020-10646
Идентификатор программной ошибки	CWE-787: Запись за границами буфера CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного VPR файла. Уязвимость обусловлена некорректной проверкой длины предоставленных пользователем данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Fuji Electric V-Server Lite до v4.0.9.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 апреля 2020 г.
Дата обновления	13 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
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.zerodayinitiative.com/advisories/ZDI-20-452/ https://nvd.nist.gov/vuln/detail/CVE-2020-10646