НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211021.7 | 21 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Fuji Electric Alpha5

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Alpha5 Smart Loader: все версии
Дата выявления	18 октября 2021 г.
Дата обновления	18 октября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8
Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

Ссылки на источники	http://www.zerodayinitiative.com/advisories/ZDI-21-1209/ http://www.zerodayinitiative.com/advisories/ZDI-21-1210/ http://www.zerodayinitiative.com/advisories/ZDI-21-1208/ https://www.cybersecurity-help.cz/vdb/SB2021101803