

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211119.16 | 19 ноября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **НЕТ**

Множественные уязвимости в FATEK Automation WinProladder

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	PLC WinProladder: 3.30_24518
Дата выявления	18 ноября 2021 г.
Дата обновления	18 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43554	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке файлов проекта.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами</p>	8.8

MITRE: CVE-2021-43556	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке файлов проекта.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами</p>	8.8
--------------------------	--	-----

Ссылки на источники	<p>https://www.cybersecurity-help.cz/vdb/SB2021111816</p> <p>http://ics-cert.us-cert.gov/advisories/icsa-21-320-01</p>
---------------------	---