# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220110.7 | 10 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

## Множественные уязвимости в WECON LeviStudioU

| | |
|---|---|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | WECON LeviStudioU: 2019-09-21 |
| Дата выявления | 4 января 2022 г. |
| Дата обновления | 4 января 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE: CVE-2021-23138 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-121: Переполнение буфера в стеке<br>Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами | 8.8 |

| | | |
|---|---|---|
| MITRE:<br>CVE-2021-23157 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-122: Переполнение буфера в динамической памяти<br>Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами | 8.8 |

| | |
|---|---|
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2022010401<br>http://ics-cert.us-cert.gov/advisories/icsa-21-355-03 |