# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220727.23 | 27 июля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в ICONICS Product Suite

| | |
|---|---|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | GENESIS64: 10.97 - 10.97.1<br>MobileHMI: 10.97 - 10.97.1<br>IoTWorX: 10.97 - 10.97.1 |
| Дата выявления | 25 июля 2022 г. |
| Дата обновления | 25 июля 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE: CVE-2022-29834 | Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C<br>CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) | 7.5 |

| | | |
|---|---|---|
| | Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. | |
| MITRE:<br>CVE-2022-33315<br>CVE-2022-33316<br>CVE-2022-33320 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br>CWE-502: Десериализация недоверенных данных<br>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. | 8.8 |
| MITRE:<br>CVE-2022-33317 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена использованием функций из недоверенных источников.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br>CWE-829: Использование функций недоверенных источников<br>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. | 8.8 |
| MITRE:<br>CVE-2022-33318 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br>CWE-502: Десериализация недоверенных данных<br>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. | 9.8 |

| | | |
|---|---|---|
| MITRE: CVE-2022-33319 | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена граничным условием в функции.<br><br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:U/RL:O/RC:C<br><br>CWE-125: Чтение за пределами буфера<br><br>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. | 8.2 |

| | |
|---|---|
| Ссылки на источники | http://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-008_en.pdf<br>http://jvn.jp/vu/JVNVU96480474/index.html |