НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220124.34 | 24 января 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ICONICS Suite

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ICONICS Suite: 10.95.3, 10.97 GENESIS64: 10.95.3, 10.97 Hyper Historian: 10.95.3, 10.97 Energy AnalytiX: 10.95.3, 10.97 MobileHMI: 10.95.3, 10.97
Дата выявления	21 января 2022 г.
Дата обновления	21 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-23128	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена неполным списком запрещенных входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-184: Неполный черный список Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2022-23129	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику просмотреть файл конфигурации. Уязвимость обусловлена некорректным хранением учетных данных. CVSSv3.0: AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-256: Хранение пароля в незашифрованном виде Рекомендации по устранению: обновить программное обеспечение	7.7

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022012107 http://iconics.com/Support/CERT http://ics-cert.us-cert.gov/advisories/icsa-22-020-01