НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221202.2 | 2 декабря 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Mitsubishi Electric FA Engineering Software

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	GX Works3: 1.000A - 1.087R MX OPC UA Module Configurator-R: все версии
Дата выявления	30 ноября 2022 г.
Дата обновления	30 ноября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-25164	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена хранением конфиденциальной информации в открытом виде. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N CWE-312: Хранение важных данных в незашифрованном виде Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.6

MITRE: CVE-2022-29830	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена использованием жестко закодированного ключа шифрования. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N CWE-321: Использование жестко закодированного ключа шифрования Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	9.1
MITRE: CVE-2022-29831	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить сведения о модуле безопасности центрального процессора. Уязвимость обусловлена наличием жестко запрограммированного пароля. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CWE-259: Использование жестко закодированного пароля Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	7.5

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-22-333-05