НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210810.5 | 10 августа 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в mySCADA myPRO

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	myPRO: до v8.20.0
Дата выявления	6 августа 2021 г.
Дата обновления	6 августа 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-33013	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным ограничением доступа для чтения системной информации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение	8.2

MITRE: CVE-2021-33009	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и запустить произвольный файл в целевой системе. Уязвимость обусловлена некорректной проверкой типа загружаемого файла. 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-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-33005	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить произвольный файл в произвольный каталог в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-27505	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить список имён каталогов в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным ограничением доступа для чтения системной информации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение важной информации лицам без соответствующих прав Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	https://ics-cert.us-cert.gov/advisories/icsa-21-217-03 https://www.cybersecurity-help.cz/vdb/SB2021080605