НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210317.5 | 17 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в IGSS SCADA

Идентификатор уязвимости	MITRE: CVE-2021-22709 CVE-2021-22710 CVE-2021-22711 CVE-2021-22712
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством импорта вредоносного CGF-файла. Уязвимость обусловлена некорректной обработкой конфигурационных файлов компонентом IGSS Definition.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IGSS SCADA:15.0.0.21041
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 марта 2021 г.
Дата обновления	15 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)

Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021031508 https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-068-01 https://www.se.com/ww/en/download/document/SEVD-2021-068-01