НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211217.40 | 17 декабря 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в WebHMI portal

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	WebHMI: до 4.1
Дата выявления	6 декабря 2021 г.
Дата обновления	6 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43936	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных файлов. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение	10.0

MITRE: CVE-2021-43931	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой механизма аутентификации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-305: Обход аутентификации с помощью стороннего недостатка Рекомендации по устранению: обновить программное обеспечение	9.8

Ссылки на источники	https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03