

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211206.10 | 6 декабря 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Distributed Data Systems WebHMI

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	WebHMI: до 4.1
Дата выявления	3 декабря 2021 г.
Дата обновления	3 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43931	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению. Уязвимость обусловлена некорректной работой процесса аутентификации.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-287: Некорректная аутентификация</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	9.8

MITRE: CVE-2021-43936	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и запустить произвольный файл в целевой системе. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/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	10.0
--------------------------	---	------

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-21-336-03 https://www.cybersecurity-help.cz/vdb/SB2021120322
---------------------	--