НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211007.1 | 7 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Emerson WirelessHART Gateway

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	WirelessHART 1420 Gateway: до 4.7.94, 4.7.105 WirelessHART 1410D Gateway: до 4.7.94, 4.7.105 WirelessHART 1410 Gateway: до 4.7.94, 4.7.105
Дата выявления	21 июня 2021 г.
Дата обновления	21 июня 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-22439	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-502: Десериализация недоверенных данных Рекомендации по устранению: обновить программное обеспечение	8.1

MITRE: CVE-2021-85337	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить доступ к другим учетным записям и изменить их настройки в целевой системе. Уязвимость обусловлена отсутствием проверки разрешений на восстановление из резервной копии. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-306: Отсутствие аутентификации для критически важных функций Рекомендации по устранению: обновить программное обеспечение	8.0
MITRE: CVE-2021-03554	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в файле восстановления. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение	8.0
MITRE: CVE-2021-81019	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в парольной фразе. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	8.0

Ссылки на источники	https://ics-cert.us-cert.gov/advisories/icsa-21-278-02 https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210619-01-injection-en https://www.cybersecurity-help.cz/vdb/SB2021100609