НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220214.10 | 14 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода оболочки в маршрутизаторах ELECOM LAN

Идентификатор уязвимости	MITRE: CVE-2022-21173
Идентификатор программной ошибки	CWE-912: Скрытые функции
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды оболочки в целевой системе. Уязвимость обусловлена наличием недокументированных средств удаленного управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	WRH-300BK3: 1.05 WRH-300WH3: 1.05 WRH-300BK3-S: 1.05 WRH-300DR3-S: 1.05 WRH-300LB3-S: 1.05 WRH-300PN3-S: 1.05 WRH-300WH3-S: 1.05 WRH-300YG3-S: 1.05
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 февраля 2022 г.
Дата обновления	8 февраля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

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/SB2022020801 http://jvn.jp/en/jp/JVN17482543/index.html http://www.elecom.co.jp/news/security/20220208-02/