НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210219.1 | 19 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ConnMan

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	ConnMan: версии с 0.1 по 1.38
Дата выявления	3 февраля 2021 г.
Дата обновления	8 февраля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-26676	Эксплуатация уязвимости позволяет злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена утечками памяти в компоненте gdhcp. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-401: Удержание памяти после ее использования Рекомендации по устранению: обновить программное обеспечение.	7.4

MITRE: CVE-2021-26675	Эксплуатация уязвимости позволяет удаленному неаутентифицированному злоумышленнику выполнить произвольный код на целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании компонента dnsproxy. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021021208