# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211111.3 | 11 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Выполнение произвольного кода в маршрутизаторах NETGEAR

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2021-34947 |
| Идентификатор программной ошибки | CWE-787: Запись за границами буфера |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями пользователя root в целевой системе. Уязвимость обусловлена ошибкой границ памяти при анализе файла soap_block_table. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | R6700AX: до 1.0.5.108<br>R7800: до 1.0.2.84<br>R8900: до 1.0.5.36<br>R9000: до 1.0.5.36<br>RAX10: до 1.0.5.108<br>RAX120: до 1.2.2.24<br>RAX120v2: до 1.2.2.24<br>RAX70: до 1.0.5.108<br>RAX78: до 1.0.5.108<br>XR700: до 1.0.1.44 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 1 октября 2021 г. |
| Дата обновления | 1 октября 2021 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/SB2021100101<br>http://www.zerodayinitiative.com/advisories/ZDI-21-1116/<br>http://kb.netgear.com/000064044/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2021-0129 |