НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210928.4 | 28 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в NETGEAR

Идентификатор уязвимости	MITRE: CVE-2021-34947
Идентификатор программной ошибки	CWE: Не определен
Описание уязвимости	Уязвимость позволяет злоумышленнику из смежной сети выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректным синтаксическим анализом файла soap_block_table.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	R6700AX до версии прошивки 1.0.5.108. R7800 до версии прошивки 1.0.2.84. R8900 до версии прошивки 1.0.5.36. R9000 и до версии прошивки 1.0.5.36. RAX10 до версии прошивки 1.0.5.108. RAX120 до версии прошивки 1.2.2.24. RAX120v2 до версии прошивки 1.2.2.24. RAX70 до версии прошивки 1.0.5.108. RAX78 до версии прошивки 1.0.5.108. XR700 до версии прошивки 1.0.1.44.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 сентября 2021 г.
Дата обновления	28 сентября 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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://kb.netgear.com/000064044/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2021-0129 https://www.zerodayinitiative.com/advisories/ZDI-21-1116/