НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200810.12 | 10 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в маршрутизаторах NETGEAR

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	R6700v3 с ПО до версии 1.0.4.98
Дата выявления	28 июля 2020 г.
Дата обновления	30 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-15635	Эксплуатация уязвимости позволяет удаленному злоумышленнику, находящемуся в локальной сети, выполнить произвольный код на целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании службы «acsd». CVSSv3.1: 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

MITRE: CVE-2020-15636	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании службы «check_ra». CVSSv3.1: :N/AC:H/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.	8.1

Ссылки на источники	https://kb.netgear.com/000062128/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-R6700v3-PSV-2020-0224 https://kb.netgear.com/000062127/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-R6700v3-PSV-2020-0202