НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220713.26 | 13 июля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в NETGEAR Routers and WiFi Systems

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	RAXE500: до 1.0.8.70 RAXE450: до 1.0.8.70 XR1000: до 1.0.0.64 MK83: до 1.1.6.14 MK62: до 1.1.6.122 R6400v2: до 1.0.4.122 R7850: до 1.0.5.76 R6700v3: до 1.0.4.122 R7000P: до 1.3.3.148 R6900P: до 1.3.3.148 R8000: до 1.0.4.76 RS400: до 1.5.1.86 XR300: до 1.0.3.68 DC112A: до 1.0.0.64 R6400: до 1.0.1.76 WNDR3400v3: до 1.0.1.44 R7000: до 1.0.11.130 MR60: до 1.1.6.122 MR80: до 1.1.6.14 MS60: до 1.1.6.122 MS80: до 1.1.6.14

Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	30 июня 2022 г.
Дата обновления	30 июня 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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	http://kb.netgear.com/000065043/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-Some-Routers-and-WiFi-Systems-PSV-2021-0187