НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210414.1 | 14 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированное обновление прошивки в продуктах компании NETGEAR

Идентификатор уязвимости	MITRE: CVE-2020-35220
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети обойти ограничения безопасности и выполнить обновление прошивки в целевой системе. Уязвимость обусловлена некорректным ограничением доступа на TFTP-сервере.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Netgear JGS516PE: 2.6.0.43 Netgear GS116Ev2: 2.6.0.43
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 марта 2021 г.
Дата обновления	11 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/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)	Низкое (L)
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/SB2021031107 https://research.nccgroup.com/2021/03/08/technical-advisory-multiple-vulnerabilities-in-netgear-prosafe-plus-jgs516pe-gs116ev2-switches/