НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210414.5 | 14 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Повышение привилегий в коммутаторах Netgear ProSafe Plus JGS516PE и GS116Ev2J

Идентификатор уязвимости	MITRE: CVE-2020-35229
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети получить привилегии администратора посредством отправки запросов, использующих один аутентифицированный пакет. Уязвимость обусловлена возможностью повторного использования токена аутентификации.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	JGS516PE: 2.6.0.43 GS116Ev2: 2.6.0.43
Рекомендации по устранению	Отключить функцию удаленного управления и прекратить использование Pro Safe Plus Configuration Utility для изменения конфигурации коммутатора.
Дата выявления	11 марта 2021 г.
Дата обновления	11 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021031108 https://research.nccgroup.com/2021/03/08/technical-advisory-multiple-vulnerabilities-in-netgear-prosafe-plus-jgs516pe-gs116ev2-switches/