НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210414.4 | 14 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в коммутаторах Netgear ProSafe Plus JGS516PE и GS116Ev2

Идентификатор уязвимости	MITRE: CVE-2020-35227
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного запроса. Уязвимость обусловлена ошибкой границ памяти в функции удаления из раздела «Контроль доступа» в параметре checkedList, используемого для отправки идентификатора хоста.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	JGS516PE: 2.6.0.43 GS116Ev2: 2.6.0.43
Рекомендации по устранению	Ограничить доступ к приложению веб-управления
Дата выявления	11 марта 2021 г.
Дата обновления	11 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
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/