

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200424.1 | 24 апреля 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Обход аутентификации в маршрутизаторе Huawei AR3200

Идентификатор уязвимости	MITRE: CVE-2020-9068 Huawei: HWPSIRT-2020-04035
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и получить доступ к целевому устройству. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Huawei AR3200 с версией ПО до V200R007SPH026 и V200R009SPH021
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 апреля 2020 г.
Дата обновления	22 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.6 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H
Вектор атаки (AV)	Сетевой (N)
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)	Низкое (L)

Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Функциональная версия
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200422-01-authentication-en