НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210210.9 | 10 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в маршрутизаторах Cisco Small Business серии RV

Идентификатор уязвимости	MITRE: CVE-2021-1319 - CVE-2021-1348
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных HTTP-запросов. Уязвимость обусловлена некорректной обработкой входных данных в веб-интерфейсе управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	RV016 Multi-WAN VPN Routers v4.2.3.14 и ранее RV042 Dual WAN VPN Routers v4.2.3.14 и ранее RV042G Dual Gigabit WAN VPN Routers v4.2.3.14 и ранее RV082 Dual WAN VPN Routers v4.2.3.14 и ранее RV320 Dual Gigabit WAN VPN Routers v1.5.1.11 и ранее RV325 Dual Gigabit WAN VPN Routers v1.5.1.11 и ранее
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 февраля 2021 г.
Дата обновления	3 февраля 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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj