НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210125.5 | 25 января 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в панели управления маршрутизаторов Cisco Small Business серии RV

Идентификатор уязвимости	MITRE: CVE-2021-1159 - CVE-2021-1217 CVE-2021-1307 CVE-2021-1360
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимостей позволяет аутентифицированному удалённому злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимости обусловлены некорректной обработкой HTTP-запросов в веб-панели управления уязвимого устройства.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Оборудование серии RV
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 января 2021 г.
Дата обновления	14 января 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)	Низкий (L)
Необходимый уровень привилегий (PR)	Высокий (H)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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-WUnUgv4U