НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200623.8| 23 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в маршрутизаторах Cisco Small Business серии RV

Идентификатор уязвимости	MITRE: CVE-2020-3274 CVE-2020-3275 CVE-2020-3276 CVE-2020-3277 CVE-2020-3278 CVE-2020-3279
Идентификатор программной ошибки	CWE-77: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных вредоносных запросов. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	RV016 Multi-WAN VPN с ПО v4.2.3.10 RV042 Dual WAN VPN с ПО v4.2.3.10 RV042G Dual Gigabit WAN VPN с ПО v4.2.3.10 RV082 Dual WAN VPN с ПО v4.2.3.10 RV320 Dual Gigabit WAN VPN с ПО v1.5.1.05 RV325 Dual Gigabit WAN VPN с ПО v1.5.1.05
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 июня 2020 г.
Дата обновления	17 июня 2020 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-routers-Rj5JRfF8