НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220812.8 | 12 августа 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Small Business RV Series Routers

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	RV160 VPN Router : 1.0.01.05 RV160W Wireless-AC VPN Router : 1.0.01.05 RV260 VPN Router : 1.0.01.05 RV260P VPN Router with PoE : 1.0.01.05 RV260W Wireless-AC VPN Router : 1.0.01.05 RV340 Dual WAN Gigabit VPN Router : 1.0.03.26 RV340W Dual WAN Gigabit Wireless-AC VPN Router : 1.0.03.26 RV345 Dual WAN Gigabit VPN Router : 1.0.03.26 RV345P Dual WAN Gigabit POE VPN Router : 1.0.03.26
Дата выявления	4 августа 2022 г.
Дата обновления	4 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-20827 CVE-2022-20841	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	9.0

	CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд) Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	
MITRE: CVE-2022-20842	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.8

Ссылки на источники	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR