НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210824.3 | 24 августа 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в маршрутизаторах Cisco

Идентификатор уязвимости	MITRE: CVE-2021-34730
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных UPnP-запросов. Уязвимость обусловлена ошибкой границ памяти в службе Universal Plug-and-Play (UPnP).
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	RV110W Wireless-N VPN Firewall: 1.0.0.2, 1.0.1.6, 1.0.3.55, 1.1.0.9, 1.2.0.9, 1.2.0.10, 1.2.1.4, 1.2.1.6, 1.2.1.7, 1.2.2.1, 1.2.2.5, 1.2.2.8, 1.3.1.7 RV130W Wireless-N Multifunction VPN Router: 1.0.0.21, 1.0.1.2, 1.0.1.3, 1.0.2.7, 1.0.3.8, 1.0.3.14, 1.0.3.15, 1.0.3.16, 1.0.3.22, 1.0.3.28, 1.0.3.44, 1.0.3.45, 1.0.3.51, 1.0.3.54, 1.0.3.55, 1.2.2.5, 1.2.2.8, 1.3.1.7 RV130 VPN Router: 1.0.3.55, 1.2.2.8, 1.3.1.7 Cisco Small Business RV130 Series VPN Routers: 1.0.0.21, 1.0.1.3, 1.0.2.7, 1.0.3.14, 1.0.3.16, 1.0.3.22, 1.0.3.28, 1.0.3.44, 1.0.3.45, 1.0.3.51, 1.0.3.52, 1.0.3.54, 1.0.3.55, 1.2.2.5, 1.2.2.8, 1.3.1.7 RV215W Wireless-N VPN Router: 1.0.3.55, 1.1.0.5, 1.1.0.6, 1.2.0.14, 1.2.0.15, 1.2.2.5, 1.2.2.8, 1.3, 1.3.0.7, 1.3.0.8, 1.3.1.1, 1.3.1.4, 1.3.1.5, 1.3.1.7
Рекомендации по устранению	Поддержка маршрутизаторов Cisco Small Business RV110W, RV130, RV130W и RV215W прекращена. Для устранения уязвимости компания Cisco рекомендует отключить поддержку UPnP на LAN интерфейсе устройства.

	Для этого посредством веб-интерфейса управления выберите раздел «Основные настройки / UPnP» и установите флажок «Отключить».
Дата выявления	18 августа 2021 г.
Дата обновления	18 августа 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	Отсутствует (N)
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	Временное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021082201 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz05607