НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200727.8 | 27 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Small Business RV110W, RV130, RV130W, RV215W Routers

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	RV110W Wireless-N VPN Firewall: 1.2.2.5 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, 1.2.2.5, 1.2.2.8 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, 1.2.2.5, 1.2.2.8 RV215W Wireless-N VPN Router: 1.3.1.4
Дата выявления	15 июля 2020 г.
Дата обновления	22 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3323 CVE-2020-3331	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных в веб-интерфейсе управления. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	9.8

	CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	
MITRE: CVE-2020-3300	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством использования жестко закодированных учетных данных. Уязвимость обусловлена наличием жестко закодированных учетных данных в программной реализации сервиса Telnet. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: обновить программное обеспечение.	9.8

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-AQKREqp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-code-exec-wH3BNFb https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv110w-static-cred-BMTWBWTy