НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ
Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ
VULN-20210210.6 | 10 февраля 2021 г.
Уровень опасности: КРИТИЧЕСКИЙ
Наличие обновления: ЕСТЬ

Множественные уязвимости в роутерах Cisco Small Business

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Роутеры с версией ПО до 1.0.01.02: RV160 VPN Router RV160W Wireless-AC VPN Router RV260 VPN Router RV260P VPN Router with POE RV260W Wireless-AC VPN Router
Дата выявления	3 февраля 2021 г.
Дата обновления	3 февраля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-1289 CVE-2021-1290 CVE-2021-1291 CVE-2021-1292 CVE-2021-1293 CVE-2021-1294 CVE-2021-1295	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной проверкой входных данных. 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-472: Возможность изменения извне предположительно неизменяемых веб-параметров Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2021-1296 CVE-2021-1297	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством подмены пути при загрузке файлов через веб-интерфейс. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C CWE-36: Подмена абсолютного пути Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn