НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200921.3| 21 сентября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Small Business RV340

Идентификатор уязвимости	MITRE: CVE-2020-3451 CVE-2020-3453
Идентификатор программной ошибки	CWE-119: Переполнение буфера в динамической памяти CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на уязвимом устройстве посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной обработкой входных данных в веб-интерфейсе управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Small Business серии RV340
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 сентября 2020 г.
Дата обновления	16 сентября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
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)	Низкое (L)

Влияние на целостность (I)	Низкое (L)
Влияние на доступность (A)	Низкое (L)
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-osinj-rce-pwTkPCJv