НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210514.2 | 14 мая 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Раскрытие содержания информации в Cisco Small Business

Идентификатор уязвимости	MITRE: CVE-2021-1400
Идентификатор программной ошибки	CWE-269: Некорректное управление привилегиями
Описание уязвимости	Эксплуатация уязвимостей позволяет удаленному аутентифицированному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной обработкой входящих HTTP-запросов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Small Business 100 серии Cisco Small Business 300 серии Cisco Small Business 500 серии
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 мая 2021 г.
Дата обновления	5 мая 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/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)	Низкий (L)
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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-ZAfKGXhF