НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210527.2| 27 мая 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Cisco Small Business 100 Series Wireless Access Points

Идентификатор уязвимости	MITRE: CVE-2021-1401
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных HTTP-запросов в веб-интерфейс управления маршрутизатора. Уязвимость обусловлена некорректной проверкой вводимых данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Small Business 100 Series Wireless Access Points: All versions Cisco Small Business 300 Series Wireless Access Points: All versions Cisco Small Business 500 Series Wireless Access Points: All versions Cisco WAP125 Wireless-AC Dual Band Desktop Access Point with PoE: 1.0.3.1 WAP131 Wireless-N Dual Radio Access Point with PoE: 1.0.2.17 Cisco WAP150 Wireless-AC/N Dual Radio Access Point with PoE: 1.1.2.4 WAP351 Wireless-N Dual Radio Access Point with 5-Port Switch: 1.0.2.17 Cisco WAP361 Wireless-AC/N Dual Radio Wall Plate Access Point with PoE: 1.1.2.4

	Cisco WAP581 Wireless-AC Dual Radio Wave 2 Access Point: 1.0.3.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 мая 2021 г.
Дата обновления	6 мая 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/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)	Высокий (H)
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://www.cybersecurity-help.cz/vdb/SB2021050631 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-ZAfKGXhF