НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220419.18 | 19 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

НСД в Cisco Wireless LAN Controller

Идентификатор уязвимости	MITRE: CVE-2022-20695
Идентификатор программной ошибки	CWE-303: Некорректная реализация алгоритма аутентификации
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректным алгоритмом проверки аутентификационных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Wireless LAN Controller Software: 8.10.151.0 - 8.10.162.0 3504 Wireless Controller: все версии 5520 Wireless Controller: все версии 8540 Wireless Controller: все версии Cisco Mobility Express: все версии Virtual Wireless Controller: все версии
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	14 апреля 2022 г.
Дата обновления	14 апреля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
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)	Изменяется (C)
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	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-auth-bypass-JRNhV4fF