НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200424.8 | 24 апреля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании Cisco Wireless LAN Controller CAPWAP

Идентификатор уязвимости	MITRE: CVE-2020-3162
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании путем отправки специально сформированного пакета протокола CAPWAP. Уязвимость обусловлена некорректной обработкой пакетов протокола CAPWAP.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco Wireless LAN Controller версий 8.5, 8.6, 8.7, 8.8, 8.9 и 8.10
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 апреля 2020 г.
Дата обновления	16 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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)	Не требуется (N)

Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
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-wlc-capwap-dos-Y2sD9uEw