НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210419.3 | 19 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в продуктах компании Cisco

Идентификатор уязвимости	MITRE: CVE-2021-1373
Идентификатор программной ошибки	CWE-125: Чтение за пределами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально созданного вредоносного CAPWAP-пакета. Уязвимость обусловлена некорректной проверкой CAPWAP-пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XE: 16.12 Cisco Catalyst 9800 Wireless Controller Embedded Wireless Controller on Catalyst Access Points Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500 Series Switches
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 марта 2021 г.
Дата обновления	29 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
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)	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://www.cybersecurity-help.cz/vdb/SB2021032920 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-capwap-dos-2OA3JgKS