



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.13 | 23 сентября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Cisco IOS XE контроллеров Catalyst серии 9800

Идентификатор уязвимости	MITRE: CVE-2021-34767
Идентификатор программной ошибки	CWE-670: Уязвимости, связанные с управлением ресурсами
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети вызвать отказ в обслуживании интерфейса целевой системы обслуживающего определенный VLAN посредством отправки IPv6 пакетов. Уязвимость обусловлена некорректной обработкой трафика IPv6.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Catalyst 9800 Wireless Controllers Catalyst 9800 Wireless Controllers для облака
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 сентября 2021 г.
Дата обновления	22 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.4 AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Смежная сеть (A)
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-ipv6-dos-NMYeCnZv