НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210909.3 | 9 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco IOS XR

Идентификатор уязвимости	MITRE: CVE-2021-34720
Идентификатор программной ошибки	CWE-771: Отсутствие ссылки на активный выделенный ресурс
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных в функциях IP Service Level Agreements (IP SLA) и Two-Way Active Measurement Protocol (TWAMP)
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	NCS540: Все версии ASR9K-PX: Все версии Cisco IOS XR: 5.3.0, 6.0, 6.1, 6.2.1, 6.2.2, 6.3.1, 6.5.2, 6.5.3, 6.6, 6.7, 7.0, 7.1, 7.2.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 сентября 2021 г.
Дата обновления	9 сентября 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/SB2021090911 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsla-ZA3SRrpP