НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210909.1 | 9 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco IOS XR в маршрутизаторах Cisco ASR 9000

Идентификатор уязвимости	MITRE: CVE-2021-34713
Идентификатор программной ошибки	CWE-399: Уязвимости, связанные с управлением ресурсами
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной обработкой пакетов канального уровня.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco ASR 9000 Series Aggregation Services Routers: 6.4, 6.4.1, 6.4.2, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.6, 6.6.1, 6.6.2, 6.7, 7.0, 7.0.1, 7.1 Cisco ASR 9001 Router: Все версии
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 сентября 2021 г.
Дата обновления	9 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	Изменяется (C)

уязвимости (S)	
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/SB2021090906 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npspin-QYpwdhFD