НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201117.1 | 17 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco ASR 9000

Идентификатор уязвимости	MITRE:	CVE-2020-26070
Идентификатор программной ошибки	CWE-404:	Некорректное освобождение ресурсов
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки потока специально сформированных протокольных блоков данных (PDUs) по протоколам 2 или 3 уровня. Уязвимость обусловлена некорректным распределением внутренних ресурсов при обработке сетевого трафика.	
Категория уязвимого продукта	Телекоммуникационное оборудование	
Уязвимый продукт	Cisco IOS XR до v6.7.2, 7.1.2 для маршрутизаторов серии Cisco ASR 9000	
Рекомендации по устранению	Обновить программное обеспечение	
Дата выявления	10 ноября 2020 г.	
Дата обновления	11 ноября 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	
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cp-dos-ej8VB9QY