

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.12 | 23 сентября 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Переполнение буфера в Cisco IOS XE SD-WAN

Идентификатор уязвимости	MITRE: CVE-2021-34727
Идентификатор программной ошибки	CWE-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды или вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	1000 Series Integrated Services Routers (ISRs) 4000 Series ISRs ASR 1000 Series Aggregation Services Routers Cloud Services Router 1000V Series
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 сентября 2021 г.
Дата обновления	22 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
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-iosxesdwan-rbuffer-vE2OB6tp>