НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210210.5 | 10 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco IOS XR Software

Идентификатор уязвимости	MITRE: CVE-2021-1268
Идентификатор программной ошибки	CWE-1076: Класс со слишком глубоким наследованием
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику, находящемуся в смежной сети, вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных IPv6-пакетов. Уязвимость обусловлена некорректным перенаправлением IPv6-трафика.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Релизы 6.3.1, 6.5.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 февраля 2021 г.
Дата обновления	3 февраля 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-xripv6-spJem78K#fs