НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.6 | 23 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco IOS и IOS XE

Идентификатор уязвимости	MITRE: CVE-2021-1620
Идентификатор программной ошибки	CWE-563: Назначение неиспользуемой переменной
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системы посредством многократных попыток подключения к устройству. Уязвимость обусловлена некорректным освобождением выделенных IP-адресов при подключении к устройству без использования Cisco AnyConnect.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS иIOS XE с включённой функцией автоматического переподключения IKEv2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 сентября 2021 г.
Дата обновления	22 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.7 AV:N/AC:L/PR:L/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)	Низкий (L)
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-ikev2-ebFrwMPr