НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.5 | 23 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход аутентификации в Cisco IOS XE

Идентификатор уязвимости	MITRE: CVE-2021-1619
Идентификатор программной ошибки	CWE-824: Обращение к неинициализированному указателю
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику изменить конфигурацию или вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных запросов. Уязвимость обусловлена обращением к неинициализированному указателю в функции аутентификации, авторизации и учета (AAA).
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XE Cisco IOS XE SD-WAN
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-aaa-Yx47ZT8Q