НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191216.1 | 16 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость видеосервиса в решениях Cisco TelePresence Collaboration Endpoint и Cisco RoomOS

Идентификатор уязвимости	MITRE: CVE-2019-15289 Cisco: cisco-sa-20191106-telepres-roomos-dos
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному неаутентифицированному злоумышленнику вызвать сбой видеосервиса и отказ в обслуживании на целевом устройстве путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной проверкой вводимых данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Cisco TelePresence CE версии до 9.8.0 Cisco RoomOS версии до July Drop 1 2019: Webex Board 55 Webex Board 55S Webex Board 70 Webex Board 70S Webex Board 85S
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	6 ноября 2019 г.
Дата обновления	6 ноября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
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)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-dos