НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.5 | 7 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение команд в ПО Cisco Webex Video Mesh

Идентификатор уязвимости	MITRE: CVE-2019-16005 Cisco: cisco-sa-20200108-webex-video
Идентификатор программной ошибки	CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику с правами администратора в приложении выполнить произвольные команды в хостовой операционной системе от имени суперпользователя посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе.
Категория уязвимого продукта	Телекоммуникационные оборудование
Уязвимое ПО	Cisco Webex Video Mesh v2019.09.19.1956m и ранее
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 января 2020 г.
Дата обновления	28 января 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
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 (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-20200108-webex-video