НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200619.1 | 19 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ к данным в Cisco Webex Meetings и Cisco Webex Meetings Server

Идентификатор уязвимости	MITRE: CVE-2020-3361
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным в целевой системе посредством отправки специально созданного вредоносного запроса. Уязвимость обусловлена некорректной обработкой токенов аутентификации уязвимым сайтом Webex.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Cisco Webex Meetings WBS 39.5.25, WBS 40.4.10, WBS 40.6.0 Cisco Webex Meetings Server v4.0 MR3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 июня 2020 г.
Дата обновления	17 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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-webex-token-zPvEjKN