# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201015.4| 15 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Подмена DLL-файлов в Cisco Webex Teams Client for Windows

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-3535 |
| Идентификатор программной ошибки | CWE-427: Неконтролируемый элемент пути поиска |
| Описание уязвимости | Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством размещения специально сформированного вредоносного DLL-файла в определенном месте. Уязвимость обусловлена некорректным функционированием механизма загрузки DLL-файлов. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Cisco Webex Teams for Windows v3.0.13464.0 – v3.0.16040.0 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 7 октября 2020 г. |
| Дата обновления | 13 октября 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Вектор атаки (AV) | Локальный (L) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Низкий (L) |
| 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-teams-dll-drsnH5AN |