НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200619.3 | 19 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполенние произвольный файлов в Cisco Webex Meetings Desktop

Идентификатор уязвимости	MITRE: CVE-2020-3263
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику запустить произвольный файл в целевой системе посредством открытия пользователем специально созданного вредоносного URL-адреса. Уязвимость обусловлена некорректной проверкой входных данных при обработке URL-адреса.
Категория уязвимого продукта	Прикладое програмное обеспечение
Уязвимое ПО	Cisco Webex Meetings Desktop до v40.1.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 июня 2020 г.
Дата обновления	17 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:H/PR:N/UI:R/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)	Требуется (R)
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-client-url-fcmpdfVY