НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190808.5 | 8 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Уязвимость протокола Cisco Discovery Protocol (CDP) в ПО Cisco TelePresence Codec (TC) и Collaboration Endpoint (CE)

Идентификатор уязвимости	MITRE: CVE-2019-1878 CISCO: cisco-sa-20190619-tele-shell-inj BDU: 2019-02216
Описание уязвимости	Эксплуатация уязвимости позволяет неаутентифицированному злоумышленнику из смежной сети выполнить произвольный код посредством отправки специально созданных пакетов CDP на уязвимое устройство. Уязвимость обусловлена недостаточной проверкой данных в полученных пакетах CDP.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Cisco TelePresence CE v8.0.0 до v8.3.7 Cisco TelePresence CE v9.1.0 до v9.5.3 Cisco TelePresence CE v9.6.0 до v9.6.3 Cisco TelePresence TC v7.0.0 до v7.3.17
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 июня 2019 г.
Дата обновления	27 июня 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
Вектор атаки (AV)	Смежная сеть (A)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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)	Не определено (X)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://nvd.nist.gov/vuln/detail/CVE-2019-1878 http://www.securityfocus.com/bid/108883 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-tele-shell-inj