НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200424.9 | 24 апреля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода и отказ в обслуживании Cisco IP Phones Web Server

Идентификатор уязвимости	MITRE: CVE-2020-3161
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе или вызвать отказ в обслуживании путем отправки специально сформированного HTTP-запроса на веб-сервер IP-телефонов Cisco. Уязвимость обусловлена некорректной обработкой HTTP-запросов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое оборудование	IP Phone 7811, 7821, 7841, и 7861 Desktop Phones IP Phone 8811, 8841, 8845, 8851, 8861, и 8865 Desktop Phones Unified IP Conference Phone 8831 Wireless IP Phone 8821 и 8821-EX
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 апреля 2020 г.
Дата обновления	16 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	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	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-voip-phones-rce-dos-rB6EeRXs