НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201106.5 | 6 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco IP Phone

Идентификатор уязвимости	MITRE: CVE-2020-3574
Идентификатор программной ошибки	CWE-371: Уязвимости, связанные с состоянием
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных TCP-пакетов. Уязвимость обусловлена некорректной обработкой TCP-пакетов.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	IP DECT 210 Multi-Cell Base Station, IP DECT 6825 с ПО до версии 4.8.1 IP Phone 8811 Series, IP Phone 8841 Series, IP Phone 8851 Series, IP Phone 8861 Series с ПО до версии 11.3.2 Unified IP Conference Phone 8831 for Third-Party Call Control Webex Room Phone с ПО до версии 1.2.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	4 ноября 2020 г.
Дата обновления	4 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
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)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
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-phone-flood-dos-YnU9EXOv