# НКЦКИ

**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

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

**УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ**

**VULN-20190806.9 | 6 августа 2019 г.**

**Уровень опасности: СРЕДНИЙ**

## Отказ в обслуживании IP-телефонов Cisco серии 7800 и 8800

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2019-1922<br>CISCO: cisco-sa-20190703-ip-phone-sip-dos<br>BDU: 2019-02539 |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена недостаточной проверкой входных данных в сетевых пакетах по протоколу SIP. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимые системы и программное обеспечение | IP Conference Phone 7832<br>IP Conference Phone 8832<br>IP Phone 7800 Series с Multiplatform Firmware<br>IP Phone 7811<br>IP Phone 7821<br>IP Phone 7841<br>IP Phone 7861<br>IP Phone 8800 Series<br>IP Phone 8800 Series – VPN feature<br>IP Phone 8811<br>IP Phone 8841<br>IP Phone 8845<br>IP Phone 8845 с Multiplatform Firmware<br>IP Phone 8851<br>IP Phone 8861<br>IP Phone 8865<br>IP Phone 8865 с Multiplatform Firmware |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 5 июля 2019 г. |
| Дата обновления | 17 июля 2019 г. |

| | |
|---|---|
| Оценка критичности уязвимости (CVSSv3) | 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:X/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) | Отсутствует (N) |
| Влияние на целостность (I) | Низкое (L) |
| Влияние на доступность (A) | Отсутствует (N) |
| 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-2019-1844<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-esa-bypass<br>http://www.securityfocus.com/bid/108149 |