# НКЦКИ

**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

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

**УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ**

**VULN-20190813.3 | 13 августа 2019 г.**

**Уровень опасности: ВЫСОКИЙ**

## Выполнение произвольных команд в коммутаторах Cisco Small Business

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2019-1914<br>CISCO: cisco-sa-20190806-sb220-inject |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнять произвольные команды с привилегиями суперпользователя на целевом устройстве посредством отправки специально сформированных вредоносных HTTP(S)-пакетов. Уязвимость обусловлена недостаточной проверкой вводимых пользователем данных. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимые системы и программное обеспечение | Коммутаторы Cisco Small Business серии 220 с ПО до v1.1.4.4 с включенным веб-интерфейсом управления. |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 6 августа 2019 г. |
| Дата обновления | 9 августа 2019 г. |
| Оценка критичности уязвимости (CVSSv3) | 7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Высокий (H) |
| 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://www.securitylab.ru/news/500339.php<br>https://nvd.nist.gov/vuln/detail/CVE-2019-1914<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-inject |