# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.9 | 23 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Отказ в обслуживании в Cisco cBR-8 Converged Broadband

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2021-1623 |
| Идентификатор программной ошибки | CWE-399: Уязвимости, связанные с управлением ресурсами |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системе посредством отправки большого количества запросов Simple Network Management Protocol (SNMP). Уязвимость обусловлена некорректным управлением внутренними ресурсами в функции обработки сообщений протокола SNMP. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | Cisco cBR-8 Converged Broadband: все версии<br>Cisco IOS XE: 16.12, 16.12.1 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 23 сентября 2021 г. |
| Дата обновления | 23 сентября 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Низкий (L) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации | Изменяется (C) |

| | |
|---|---|
| уязвимости (S) | |
| 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-cbr8snmp-zGjkZ9Fc |