

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210923.10 | 23 сентября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Cisco IOS XE

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2021-1624 |
| Идентификатор программной ошибки | CWE-399: Уязвимости, связанные с управлением ресурсами |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки большого потока сетевых пакетов. Уязвимость обусловлена некорректным использованием функции ограничения скорости в процессоре Cisco QuantumFlow. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | Cisco IOS XE, если включена функция NAT с ограничением скорости |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 22 сентября 2021 г. |
| Дата обновления | 22 сентября 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.6 AV:N/AC:L/PR:N/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) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Изменяется (C) |
| 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-ratenat-pYVLA7wM |