НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Угроза эксплуатации уязвимостей в оборудовании компании Cisco

ALRT-20220303.1 | 3 марта 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Уязвимое программное обеспечение	Cisco IOS: 15.6.3 M1 - 16.5.1 Cisco IOS XE: 3.16.1aS
Описание	По каналам НКЦКИ получены сведения о массовой эксплуатации злоумышленниками уязвимостей в оборудовании компании Cisco. На данный момент активно эксплуатируются уязвимости: CVE-2017-6736 CVE-2017-6737 CVE-2017-6738 CVE-2017-6739 CVE-2017-6740 CVE-2017-6741 CVE-2017-6742 CVE-2017-6743 CVE-2017-6744 Эксплуатация указанных уязвимостей позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного SNMP-пакета. Уязвимость обусловлена некорректной проверкой входных данных. В ходе наблюдаемых компьютерных инцидентов злоумышленники используют данные уязвимости для удаления конфигурационных файлов и вывода из строя оборудования.

Уязвимости устраняются официальным патчем от вендора. Рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков и, по возможности, после проверки в тестовой среде.

Помимо обновления программного обеспечения возможно применение следующих защитных мер:

- разрешить доступ SNMP к уязвимой системе только доверенным пользователям.
- настроить CoPP фильтры.
- проверить настройки AAA (система аутентификации авторизации и учета событий).
- применить vty/snmp для acl.
- отключить следующие MIB на устройстве:
  ADSL-LINE-MIB
  ALPS-MIB
  CISCO-ADSL-DMT-LINE-MIB
  CISCO-BSTUN-MIB
  CISCO-MAC-AUTH-BYPASS-MIB
  CISCO-SLB-EXT-MIB
  CISCO-VOICE-DNIS-MIB
  CISCO-VOICE-NUMBER-EXPANSION-MIB
  TN3270E-RT-MIB

Напоминаем, что в случае, если эксплуатация уязвимостей повлекла компьютерный инцидент на объекте критической информационной инфраструктуры Российской Федерации, то его владелец (субъект КИИ) в соответствии с Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ обязан уведомить об этом НКЦКИ.

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2017070303 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp