??????? ????

Cisco Smart Install misuse

Cisco Smart Install — программа Cisco для автоматизации начальной настройки и загрузки образа операционной системы для нового оборудования Cisco. По умолчанию Cisco Smart Install активен на оборудовании Cisco и использует протокол транспортного уровня TCP с номером порта 4786.

В 2018 году в этом протоколе была обнаружена критическая уязвимость CVE-2018-0171. Уровень угрозы составляет 9,8 по шкале CVSS. Специально созданный пакет, отправленный на порт TCP/4786, на котором активен Cisco Smart Install, вызывает переполнение буфера, что позволяет:

- Принудительно перезагрузить устройство.
- Вызвать RCE.
- Похитить конфигурацию сетевого оборудования.

Для эксплуатации этой уязвимости был разработан инструмент SIET (Smart Install Exploitation Tool), который позволяет
злоупотреблять Cisco Smart Install:

```
sudo python siet.py -t -i 192.168.0.1
```

Параметры:

-t проверить устройство для интеллектуальной установки
-g получить конфигурацию устройства
-c изменить конфигурацию устройства
-C изменить несколько конфигураций устройства
-u обновить IOS устройства
-e выполнить команды в консоли устройства
-i ip-адрес целевого устройства
-l ip список целей (путь к файлу)

Обратная разработка эксплойта Mikrotik из Vault 7 CIA Leaks

ChimayRed (CR) - это эксплойт, который используется против маршрутизаторов MikroTik (MT) под управлением RouterOS.
Он используется для загрузки полезной нагрузки на маршрутизатор MT. Использует порт: tcp/80.

WinboxExploit

Это критическая уязвимость WinBox (CVE-2018-14847), которая позволяет произвольно считывать пароли из файлов
конфигурации MirkoTik. Все версии RouterOS с 2015-05-28 по 2018-04-20 уязвимы к этому эксплойту. Использует порт: tcp/8291.

Практика

Стенд: https://stepik-files.cyber-ed.space/WhiteHat/Mikrotik.ova

Логин admin пароль password

Задача - найти предыдущий пароль.

Revision #2
Created 6 October 2025 18:07:29 by Admin
Updated 7 October 2025 16:14:02 by Admin