УДК 004.056.53

Байлюк Є. М., асистент кафедри
Непша І. О., студент групи КІ-2
Житомирський державний технологічний університет

ФУНКЦІЯ POWERON AUTO PROVISIONING ДЛЯ КОМУТАТОРІВ З ОПЕРАЦІЙНОЮ СИСТЕМОЮ NEXUS

З розвитком інформаційних технологій виникає ряд проблем, які потребують своєчасного реагування та нових методів їх вирішення. Зокрема, сюди відноситься автоматизація налаштувань мережевого обладнання комп'ютерних мереж великого розміру. Її впровадження звільнює співробітників від рутинних процесів та зберігає час. Існує велика кількість функцій для обладнання різних виробників, які допомагають мережевим адміністраторам швидко розгорнути велику мережу. Розглянемо одну із них, що використовується для налаштування пристроїв з операційною системою Nexus фірми Cisco.

PowerOn Auto Provisioning (POAP) – зручна функція для автоматизації та пришвидшення процесу розгортання комутаторів з операційною системою NX-OS(OC Nexus). Вона виступає аналогом функцій Cisco Zer-Touch Provisioning та Cisco Smart Install. Дана функція доступна за замовчуванням і активується на пристроях, у яких відсутні файли стартових конфігурацій. Але нещодавно розробники компанії Cisco випустили оновлену версію NX-OS для всіх комутаторів моделі Nexus, в якій з'явилася команда для відключення POAP, а також порекомендували усім користувачам скористатися даною командою. У чому ж полягає проблема POAP?

Щоб відповісти на це питання, потрібно спочатку зрозуміти принцип роботи цієї функції. Алгоритм її роботи доволі простий: вона перевіряє наявність локального конфігураційного скрипта, і, якщо він відсутній, налаштування комутатора були обнулені або комутатор взагалі запускається вперше, POAP зв'яжеться з серверами, що були раніше додані до системного списку для того, щоб завантажити конфігураційний файл. Для виконання, описаного вище алгоритму, POAP спочатку повинен отримати IP-адресу від DHCP-сервера. Більш нові версії NX-OS також підтримують завантаження POAP з USB, якщо помістити туди необхідні файли та налаштувати іменування папок відповідним чином.

Для роботи POAP потрібна наступна мережева інфраструктура: DHCP-сервер для початкового налаштування IP-адреси, адреси шлюзу і сервера доменних імен (DNS); сервер TFTP, що містить сценарій конфігурацій, який використовується для автоматизації процесу уста-

новки і налаштування образу програмного забезпечення; один або декілька файлових серверів, які містять потрібні образи програмного забезпечення та файли конфігурацій.

Саме у DHCP приховується основна небезпека для мережі, на комутаторах якої працює ця функція. Справа у тому, що POAP використовує першу ж відповідь від DHCP-сервера, без якої-небудь ідентифікації джерела повідомлення. Цією особливістю може легко скористатися зловмисник, який захоче атакувати мережу. Він може відправити спеціально сформовану DHCP-відповідь та «змусити» комутатор завантажити конфігураційні скрипти з підконтрольного зловмиснику сервера. Така вразливість не дає можливості напряму перехоплювати контроль над комутатором, але може знадобитися для отримання доступу до інших пристроїв мережі, якщо зловмисник скомпрометував яку-небудь систему у внутрішній мережі.

Довідковий скрипт, наданий Cisco, підтримує наступні функціональні можливості:

– отримання ідентифікатору, специфічного для комутатора, наприклад, серійного номеру;

– завантаження образу програмного забезпечення, якщо файли ще не наявні на комутаторі;

– розкладка завантаженої конфігурації, яка буде застосована при наступному перезавантаженні комутатора;

– збереження конфігурації, як стартової конфігурації.

Щоб підвищити рівень захисту власної мережі, в якій працює POAP розробники з компанії Cisco рекомендують дотримуватися наступних порад:

– перевірка DHCP-повідомлень отриманих від ненадійних джерел та фільтрація повідомлень, що не пройшли перевірку;

– створення та постійне оновлення бази даних, яка містить у собі інформацію про ненадійні DHCP-сервери з орендованими IP-адресами;

– використання, раніше створеної, бази даних для перевірки запитів від вузлів.

У процесі дослідження даного питання, було з'ясовано, що POAP має ряд корисних та практичних переваг, завдяки яким масштабування мережі та налаштування комутаторів в ній значно спростилися. Але також ця функція має один суттєвий недолік, який ставить під загрозу безпеку всієї мережі.

Кожен сам повинен вирішувати для себе, що є більш важливим в різних конкретних ситуаціях: зручність та простота налаштування чи максимальний рівень захищеності системи.