CERT-UA

Рекомендації
26 листопада 2014

CUA-14-02A
Рекомендації CERT-UA для усунення вразливостей, пов’язаних з використанням протоколу SNMP

Державна служба спеціального зв’язку та захисту інформації України
Державний центр захисту інформаційно-телекомунікаційних систем
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація

1.1 Вразливі системи

- Прилади, які використовують SNMP

1.2 Інформація про протокол SNMP

SNMP (англ. Simple Network Management Protocol — простий протокол керування мережею) — це протокол керування мережами зв'язку, на основі архітектури TCP/IP. До підтримуючих SNMP пристроїв відносяться маршрутизатори, комутатори, сервери, робочі станції, принтери та інші [1].

SNMP — це технологія, покликана забезпечити керування й контроль за пристроями й прикладними програмами в мережі зв'язку шляхом обміну керуючою інформацією між агентами, що розташовуються на мережевих пристроях, і менеджерами, розташованими на станціях керування. SNMP визначає мережу як сукупність мережевих керуючих станцій й елементів мережі (головні машини, шлюзи й маршрутизатори, термінальні сервери), які спільно забезпечують адміністративні зв'язки між мережевими керуючими станціями й мережевими агентами. SNMP різних версій присвячений цілий ряд рекомендацій IETF (RFC).

Докладна реалізація протоколу й системи в цілому описана в:

- RFC 1155 (STD 16) — *Structure and Identification of Management Information for the TCP/IP-based Internets*
- RFC 1156 (Historic) — *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157 (Historic) — *A Simple Network Management Protocol (SNMP)*
- RFC 1213 (STD 17) — *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
- RFC 1452 (Informational) — *Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework* (Obsoleted by RFC 1908)
- RFC 1901 (Experimental) — *Introduction to Community-based SNMPv2*
- RFC 1902 (Draft Standard) — *Structure of Management Information for SNMPv2* (Obsoleted by RFC 2578)
- RFC 1908 (Standards Track) — *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework*
- RFC 2570 (Informational) — *Introduction to Version 3 of the Internet-standard Network Management Framework* (Obsoleted by RFC 3410)

- RFC 2578 (STD 58) — *Structure of Management Information Version 2 (SMIv2)*
- RFC 3410 (Informational) — *Introduction and Applicability Statements for Internet Standard Management Framework*
- STD 62
  - RFC 3411 — *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
  - RFC 3412 — *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
  - RFC 3413 — *Simple Network Management Protocol (SNMP) Applications*
  - RFC 3414 — *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
  - RFC 3415 — *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
  - RFC 3416 — *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
  - RFC 3417 — *Transport Mappings for the Simple Network Management Protocol (SNMP)*
  - RFC 3418 — *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 3430 (Experimental) — *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping*
- RFC 3584 (BCP 74) — *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 3826 (Proposed) — *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*
- RFC 5343 (Proposed) — *Simple Network Management Protocol (SNMP) Context EngineID Discovery*
- RFC 5590 (STD 78) — *Transport Subsystem for the Simple Network Management Protocol (SNMP)*
- RFC 5591 (STD 78) — *Transport Security Model for the Simple Network Management Protocol (SNMP)*
- RFC 5592 (Proposed) — *Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)*
- RFC 5608 (Proposed) — *Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models.*
- RFC 6353 (STD 78) — *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*

1.3 Типові вразливості SNMP

Не дивлячись на те, що протокол SNMP був реалізований великою кількістю розробників, було знайдено декілька вразливостей, які присутні майже у всіх реалізаціях протоколу, не залежно від версії та розробника. Ці вразливості можуть стати причиною:

- отримання неавторизованого привілейованого доступу
- атак відмови в обслуговувані (DoS)
- стати причиною нестабільної роботи

SNMPv1 підтримує 5 різних типів повідомлень: GetRequest, SetRequest, GetNextRequest, GetResponse, Trap. Повідомлення протоколу SNMP посилається, як Одиниця Даних Протоколу (Protocol Data Unit, PDU). Ці повідомлення описуються за допомогою Абстрактної синтаксичної нотації (Abstract Syntax Notation, ASN.1) і переводяться в бінарний формат з використанням Базових Правил Кодування (Basic Encoding Rules, BER). SNMP-менеджери та агенти повинні вміти правильно та надійно декодувати повідомлення і оброблювати отримані дані.

Вразливості в обробці повідомлень trap

SNMP trap-повідомлення відправляються від агентів до менеджерів. Trap-повідомлення вказує на попередження, або помилковий стан, в іншому випадку сповіщає менеджера про стан агенту. SNMP-менеджери повинні вміти правильно та надійно декодувати trap-повідомлення і оброблювати отримані дані. При тестуванні було знайдено декілька вразливостей в методах декодування і обробки trap-повідомлень SNMP-менеджерами [4].

Вразливості при обробці запитів

SNMP-запити посилаються від менеджерів до агентів. Запит може містити дані для отримання інформації про агента чи містити в собі інструкції для агенту з метою конфігурації якогось мережевого пристрою. SNMP-агенти, в свою чергу, повинні вміти правильно декодувати запити і оброблювати отримані дані. При тестуванні було виявлено декілька вразливостей в методах декодування і подальшої обробки запитів SNMP-агентами [3].

При виконанні тестів, які були направлені на розшифрування ASN.1 та на пошук виключень при обробці розшифрованих даних, було знайдено декілька вразливостей в декодуванні ASN.1 та наступній обробці запитів, які притаманні як менеджерам, так і агентам. Вразливості включають в себе вразливості до успішного проведення атак «відмови в обслуговувані» (DoS), вразливість публічної строки та вразливість переповнення буфера. Навіть коректна обробка SNMP-повідомлень також може стати передумовою виникнення деяких із вищеперерахованих вразливостей.

Вразливість до атак типу SNMP-amplification

Для здійснення SNMP DDoS атаки, зловмиснику потрібно володіти списком SNMP-хостів та публічних строк (community string). Зловмисник може отримати список вразливих хостів, які використовують протокол SNMP, методом сканування портів якогось діапазону IP-адрес, або зі списку відомих SNMP-хостів з приватного джерела. Значення публічних строк підбирається методом перебору паролів, так як за замовчанням в публічних строках стоять стандартні значення «public» чи «private» і більшість користувачів не поспішають їх змінювати, це зводить роботу по підбору паролів до мінімуму. Суть атаки полягає в тому, що зловмисник посилає SNMP-запит (наприклад GetBulkRequest) до якогось SNMP-хосту із заміною дійсної IP-адреси джерела запиту IP-адресою жертви атаки. Робота SNMP базується на використанні протоколу UDP, який не вимагає встановлення з'єднання і працює без збереження стану про з'єднання, тому підміна IP-адреси є можливою. SNMP-відповідь приходить на IP-адресу жертви. Оскільки розмір відповіді набагато більший за розмір запиту, атакуючий може значно збільшити розмір трафіка, спрямованого на IP-адресу жертви (Рис. 1) [6].

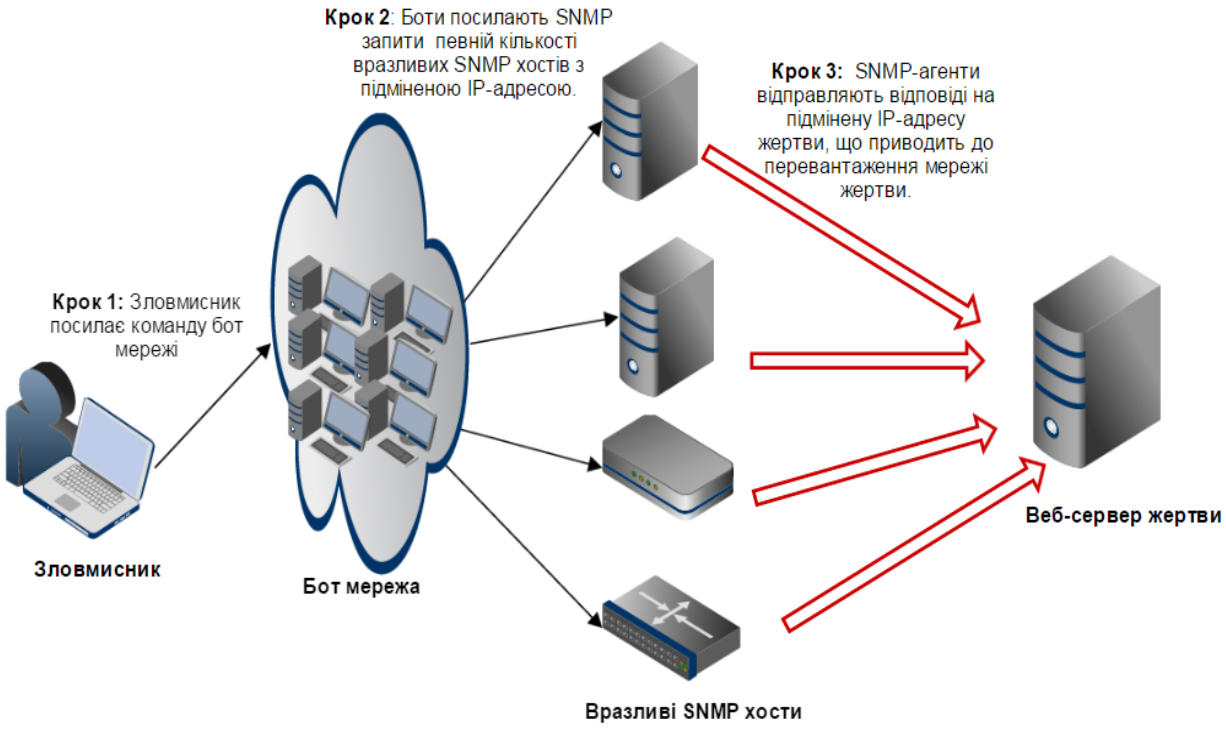

Рис. 1 Атака типу SNMP-amplification

2. Рекомендації щодо усунення вразливостей протоколу SNMP

Попередження: Описані нижче кроки можуть вплинути на роботу ваших повсякденних мережевих операцій. Впевніться що внесенні зміни, зроблені на основі рекомендацій, не будуть безпосередньо впливати на працездатність мережі [2].

Для уникнення проблем, пов'язаних з вразливостями протоколу SNMP, головною рекомендацією є відключення протоколу на всіх пристроях, якщо в ньому немає необхідності. Також рекомендується використовувати оновлення від виробників конкретної реалізації протоколу та приладів, які його використовують. Також, якщо є можливість, потрібно використовувати спеціалізоване ПО і апаратуру для збільшення надійності роботи в мережах які використовують протокол SNMP. Нижче приведені рекомендації щодо зменшення ризику використання протоколу SNMP.

Вхідна фільтрація

Можливо обмежити кількість виникаючих вразливостей шляхом блокування доступу до SNMP сервісів користувачів із зовнішньої мережі (наприклад, з Інтернету).

Використання фільтрації – це адміністративний контроль над потоком вхідного трафіка, що в свою чергу зменшує ризик виникнення загроз зі сторони зовнішньої мережі. Типова ситуація, коли сервери в мережі повинні оперувати, в основному, з трафіком з мережі Інтернет. Така фільтрація зможе обмежити доступ із зовнішньої мережі до внутрішніх сервісів. Для протоколу SNMP фільтрація вхідного трафіку, на вказаних нижче портах, дозволяє запобігти атакам зловмисників із зовнішньої мережі з метою впливу на мережеві пристрої та участі у атаках типу SNMP-amplification.

```
snmp      161/udp      # Simple Network Management Protocol (SNMP)
snmp      162/udp      # SNMP system management messages
```

Наступні порти використовуються рідкіше і присутні не у всіх реалізаціях протоколу

```
snmp                161/tcp     # Simple Network Management Protocol
(SNMP)
snmp                162/tcp     # SNMP system management messages
smux                199/tcp     # SNMP Unix Multiplexer
smux                199/udp     # SNMP Unix Multiplexer
synoptics-relay     391/tcp     # SynOptics SNMP Relay Port
synoptics-relay     391/udp     # SynOptics SNMP Relay Port
```

```
agentx              705/tcp     # AgentX
snmp-tcp-port     1993/tcp     # cisco SNMP TCP port
snmp-tcp-port     1993/udp     # cisco SNMP TCP port
```

Впевніться, що фільтрація вхідного трафіку на вказаних портах не вплине на роботу вашої мережі.

Також необхідно знати те, що в більшості реалізацій протоколу SNMP, SNMP-демон може зв'язуватися з усіма IP-інтерфейсами мережевого пристрою. Це має важливі наслідки при розгляді відповідних заходів фільтрації пакетів, необхідних для захисту приладу, який підтримує SNMP. Блокування пакетів, які поступають на одну IP-адресу не вбереже від можливої атаки на інші IP-адреси цього ж інтерфейсу. Наприклад, за рахунок використання пакетів, направлених на широкомовні (broadcast) адреси мереж (підмереж), loopback адресу (127.0.0.1). Також рекомендується блокувати доступ до RPC сервісів, які відносяться до SNMP.

```
snmp        100122 na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-
utk
snmpv2      100138 na.snmpv2      # SNM Version 2.2.2
snmpXdmid   100249
```

Зверніть увагу, що цей спосіб не може захистити вразливі прилади від внутрішніх атак.

Фільтрація SNMP трафіку від неавторизованих внутрішніх хостів

В більшості мереж тільки обмеженій кількості клієнтів, які керують мережею, необхідно передавати і оброблювати SNMP-запити. Внаслідок цього можливо налаштувати SNMP-агенти (чи мережеві пристрої між системою менеджером і системою агентом) так, щоб вони блокували запити від неавторизованих систем. Це може зменшити, але не повністю позбавити, загрозу зі сторони внутрішніх хостів. Цей метод збільшує навантаження на мережу і негативно впливає на її працездатність.

Зміна публічних строк, встановлених за замовчуванням (default community strings)

Більшість продуктів з підтримкою SNMP поставляється з встановленими за замовчуванням публічними строками доступу: «public» - доступ на зчитування, «private» - доступ на зчитування/запис. Публічна доступність сервісу та використання типових значень аутентифікаційних даних створюють передумови до використання цих хостів, як приклад, для проведення DDoS-атак або для їх компрометації. В цьому випадку рекомендується, щоб мережеві адміністратори змінювали ці строки на стійкий пароль, відмінний від значень прописаних за замовчуванням. Але навіть при зміні цих строк, якщо мережа прослуховується, можливо визначити ці строки, оскільки вони передаються в пакетах у відкритому вигляді і не шифруються (plaintext). В SNMPv3 реалізовані додаткові можливості, пов'язані з аутентифікацією, конфіденційністю і

безпекою даного протоколу в цілому (описано в RFC2574). Тому, при можливості, відмовтесь від використання SNMPv1 та SNMPv2, а використовуйте SNMPv3.

Розподілення SNMP трафіку на окремі управляючі мережі.

В ситуаціях, коли відмовитись від використання протоколу SNMP чи від блокування окремих його компонентів не є можливим, зменшення впливу вразливостей можна досягти обмеженням доступу до SNMP в межах ізольованої управляючої мережі, яка не являється публічно доступною (broadcast node). Це рекомендується робити за допомогою використання віртуальних локальних мереж (VLAN). Даний захід збільшить складність проведення атаки для зловмисника. Також, дану схему можливо реалізувати у поєднанні з механізмом побудови VPN мереж, який в свою чергу підтримує криптостійкий алгоритм аутентифікації. Ці механізми вимагають значних змін в архітектурі самої мережі.

Вихідна фільтрація

Приладам, які використовують SNMP, зазвичай, не потрібно передавати вихідний SNMP-трафік за межі локальної мережі в Інтернет. Якщо у вас також немає такої потреби, можливо реалізувати вихідну фільтрацію. Фільтрація вихідного трафіку на портах UDP 161 і 162 на виході з мережі (uplink) може попередити використання вашої системи в якості інструменту для DDoS-атаки.

3. Корисні посилання

[1] https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[2] http://www.cert.org/historical/advisories/ca-2002-03.cfm

[3] http://www.kb.cert.org/vuls/id/854306

[4] http://www.kb.cert.org/vuls/id/107186

[5] http://www.bitag.org/report-snmp-ddos-attacks.php

[6]http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf

[7] http://www.server.md/articles/73/

[8] http://www.opensnmpproject.org/

Зміни до документу

- 26.11.2014: Перший випуск