УДК 004.056:004.715
DOI: 10.31673/2409-7292.2024.020001

Савченко В. А., Бичков В. В.

ДОСЛІДЖЕННЯ ПОТЕНЦІЙНИХ УРАЗЛИВОСТЕЙ РОУТЕРІВ CISCO ДО ЗОВНІШНІХ ІН'ЄКЦІЙ

Стаття присвячена аналізу та оцінці безпеки мережевих роутерів Cisco в контексті зовнішніх ін'єкцій. Зовнішні ін'єкції - це атаки, які полягають у введенні шкідливого коду або даних в систему через зовнішні джерела. Попередні дослідження та інформація щодо уразливостей роутерів Cisco свідчать про серйозні загрози для безпеки цих пристроїв. Деякі дослідники та кібербезпекові спеціалісти вже виявили та документували різні типи атак та уразливостей, які можуть використовуватися для атак на роутери Cisco. Ці дослідження надають важливий контекст для розуміння потенційних загроз безпеці роутерів Cisco та допомагають виявити області, які потребують подальших досліджень та заходів забезпечення безпеки. В статті докладно розглядаються потенційні загрози та уразливості, яким піддаються роутери Cisco, і проводиться систематичний аналіз результатів досліджень, спрямованих на виявлення цих уразливостей. Детально розглянуті Брут-форс атака на протокол TACACS+ та зламування роутерів Cisco за допомогою SYNful Knock. Зроблено висновок щодо можливості запобігання потенційним уразливостям роутерів Cisco до зовнішніх ін'єкцій. Результати дослідження підкреслюють необхідність постійного моніторингу та підвищення безпеки мереж, які використовують роутери Cisco. Зовнішні ін'єкції можуть призвести до серйозних наслідків, включаючи втрату конфіденційності даних, порушення цілісності та доступність мережевих ресурсів. Дослідження та практичні рекомендації, надані в цій статті, можуть слугувати як основа для подальших заходів забезпечення безпеки та захисту від зовнішніх ін'єкцій у мережах, що використовують роутери Cisco.

Ключові слова: Cisco, роутер, ін'єкція, TACACS, SYNful Knock

Вступ

Мережеві роутери від компанії Cisco є ключовими компонентами сучасних інформаційних та комунікаційних мереж. Вони виконують завдання пересилання даних між різними мережами, регулюють трафік та забезпечують надійну комунікацію між комп'ютерами, серверами та іншими пристроями. Роутери Cisco відомі своєю надійністю, продуктивністю та розширюваністю, і саме тому вони широко застосовуються в корпоративних, урядових та інших критичних мережах.

Постановка проблеми

Безпека мереж є однією з найважливіших аспектів сучасних технологій. Роутери, як ключові елементи мереж, мають бути захищені від різноманітних загроз, оскільки їх уразливість може призвести до серйозних наслідків. Потенційні загрози включають атаки на роутери, які можуть призвести до втрати конфіденційності, цілісності та доступності даних. Основні загрози включають атаки на веб-додатки, атаки на протоколи маршрутизації, зламання паролів та інші методи, спрямовані на вразливості мережевого обладнання.

Аналіз публікацій

У статті [1] розглядаються абстрактні алгоритми, які складають протокол маршрутизації оптимізованого стану зв'язку версії 2 (OLSRv2), і визначаються можливі вразливості та атаки для кожного елемента протоколу – певним чином, надається «кулінарна книга» про те, як як найкраще атакувати діючу мережу OLSRv2 або як продовжити розробку захисних заходів проти цих атак. В публікації [2] автори досліджували безпеку побутових маршрутизаторів і знайшли низку критичних уразливостей. Оцінки показують, що 10 із 36 популярних маршрутизаторів уразливі до ін'єкцій підроблених записів через неправильне тлумачення спеціальних символів. Також, було виявено, що в 15 із 36 маршрутизаторів можна обійти механізми, призначені для запобігання атакам отруєння кешу. У Інтернет-дослідженні з рекламною мережею автори проаналізували 976 домашніх маршрутизаторів, які використовуються веб-клієнтами, понад 95% з яких виявилися вразливими до зазначених атак. Загалом уразливі маршрутизатори є поширеним явищем і розподілені між 177 країнами та 4830 мережами.

У [3] автори зосереджуються на важливому класі вразливостей під назвою «обхід автентифікації», які дозволяють зловмиснику отримати контроль над мережевим пристроєм,

підриваючи процедуру автентифікації. Оцінено вразливості обходу автентифікації в маршрутизаторах SOHO. Дослідження зосереджено на кількох вибраних країнах, щоб виявити наявність уразливих пристроїв. У статті [4] аналізуються як сильні, так і слабкі сторони протоколу маршрутизації OSPF з точки зору безпеки. З його сильних сторін – найменша залежність від інформації та приховування інформації, що робить його дуже надійним і стійким до збоїв, навіть якщо він стикається з певними зловмисними атаками. Слабкою стороною протоколу є можливість атаки на перемаршрутизацію, і саморобний шкідливий маршрутизатор може легко порушити роботу протоколу.

Основна мета дослідження [5] полягає в тому, щоб забезпечити комплексний огляд існуючих уразливостей у протоколах ad hoc маршрутизації, що в кінцевому підсумку забезпечує основу для захисту зв'язку в MANET. Автори показують поточні виклики та вразливі місця протоколів спеціальної маршрутизації, які призводять до труднощів у проектуванні та розробці безпечного протоколу маршрутизації. Крім того, атаки маршрутизації поділено на дві категорії, внутрішні та зовнішні, а також надаються механізми захисту від них.

Метою даної статті є дослідження потенційних уразливостей роутерів Cisco до зовнішніх ін'єкцій. Об'єктом дослідження є різні моделі роутерів Cisco, а також методи та прийоми, які можуть використовуватися для захисту від потенційних атак.

Огляд існуючих уразливостей

Зовнішні ін'єкції - це атаки, які полягають у введенні шкідливого коду або даних в систему через зовнішні джерела. У контексті безпеки веб-додатків ін'єкція відноситься до атак, при яких зловмисники вводять шкідливий код або дані в додаток через вразливість. Ін'єкції можуть призвести до небезпеки якщо не буде вчасно виявлена і запобіжна дія не буде прийнята. Такі атаки можуть впливати на конфіденційність, цілісність і доступність даних, і найбільш поширені види ін'єкцій включають SQL-ін'єкції, XSS (Cross-Site Scripting), ін'єкції команд та інші.

Попередні дослідження та інформація щодо уразливостей роутерів Cisco свідчать про серйозні загрози для безпеки цих пристроїв. Деякі дослідники та кібербезпекові спеціалісти вже виявили та документували різні типи атак та уразливостей, які можуть використовуватися для атак на роутери Cisco. Ці дослідження надають важливий контекст для розуміння потенційних загроз безпеці роутерів Cisco та допомагають виявити області, які потребують подальших досліджень та заходів забезпечення безпеки.

Методологія дослідження

Брут-форс атака на протокол TACACS+

TACACS+ – це клієнт-серверний протокол (TCP), який працює у форматі запит – відповідь (Клієнтом виступає пристрій Cisco, а сервером – сервіс TACACS +) [6]. Він підтримує шифрування трафіку за допомогою спільного ключа (Pre-Shared Key). У цьому заголовки протоколу не шифруються, тоді як тіла (дані) шифруються повністю. Зашифровані дані (enc_data) є результатом операції XOR з даними (data) і спеціальним рядком – `pseudo_pad`.

```
data^pseudo_pad=enc_data
```

де `pseudo_pad` – це послідовність хешей MD5.

```
pseudo_pad = {MD5_1 [,MD5_2 [ … ,MD5_n]]}
```

Хеші створюються на підставі даних із заголовків пакетів TACACS+ плюс загальний ключ (PSK) плюс попередній хеш (для першого MD5 його немає), рис. 1.

```
MD5_1 = MD5{session_id, key, version, seq_no}
MD5_2 = MD5{session_id, key, version, seq_no, MD5_1}
....
```

```
MD5_n = MD5{session_id, key, version, seq_no, MD5_n-1}
```

де `session_id` – випадковий ідентифікатор сесії;
`version` – версія протоколу;
`seq_no` – номер пакета, що інкрементується;
`key` – PSK.

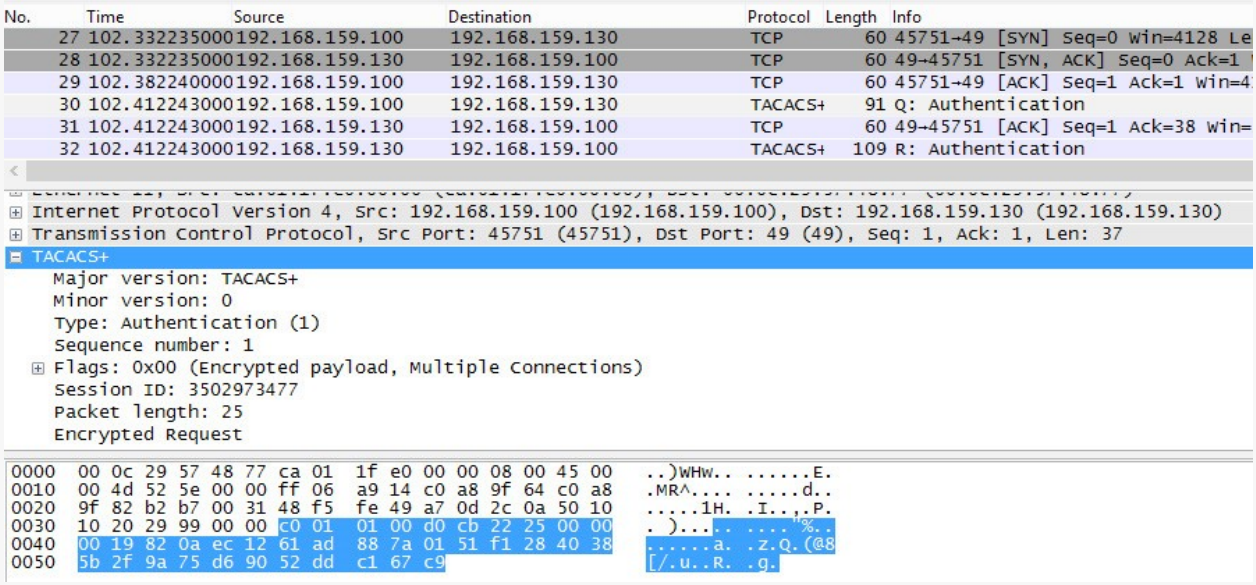

Рис. 1. Вікно контроллера

Отже, у нас є пристрій Cisco та сервер TACACS+. Ми можемо провести на них атаку Man-in-the-Middle і бачити трафік, що передається. Наша мета – отримати PSK та за допомогою нього розшифрувати трафік та отримати валідні облікі.

Для початку, як ми бачимо, значення MD5 створюється від кількох значень, але тільки одне з них точно не знаємо – загальний ключ. Решту можна отримати із заголовків TACACS+ пакета. Якщо спростити завдання, все зводиться до того, щоб перебором підібрати ключ. При цьому MD5 можна знайти в офлайні дуже швидко. Але для цього потрібно отримати значення MD5_1. Враховуючи, що значення з MD5_2 по MD5_n містять ще й попереднє значення MD5, вони для нас за великим рахунком марні (виходить друге невідоме).

Далі, необхідно згадати, що XOR – це оборотна операція. Якщо ми мали операцію `data^pseudo_pad = enc_data`, то `pseudo_pad = data^enc_data`. При цьому XOR – це найпростіша операція, і зміна частини рядка не тягне за собою зміни в іншій її частині. Отримуємо MD5_1 – це початкова частина pseudo_pad (точніше, 128 біт або 16 байт). Таким чином, щоб отримати MD5_1, нам потрібно знати перші 16 байт зашифрованих даних та 16 байт початкових даних. І якщо зашифровані дані є в будь-якій кількості з трафіку, як отримати 16 байт початкових даних?

Поглянемо на формат пакету даних користувача. Формат відрізняється для запитів і відповідей, а також для різних видів (TACACS+ – це Authentication, Authorization, Accounting). Пакет складається з кількох полів (чотири байти): Action, Priv Level, Auth Type, Service. Вони вказують на те, що хтось хоче автентифікуватись на циску. При цьому в більшості випадків вони матимуть значення 01. Далі User len, але в першому пакеті автентифікації це значення не використовується, тому 00. Далі Port len – це довжина імені терміналу, на який відбувається підключення. Для віддалених підключень має бути 04. Далі довжина IP-адреси, що підключається. Після цього – поле Data, яке теж дорівнюватиме 00 для першого пакета. Далі – Port. Це номер або ім’я терміналу Cisco-девайсу. І останнє поле – це сама IP-адреса, що

підключається (причому нас цікавлять лише чотири байти від його початку, до повних 16 байт незашифрованих даних), рис. 2.

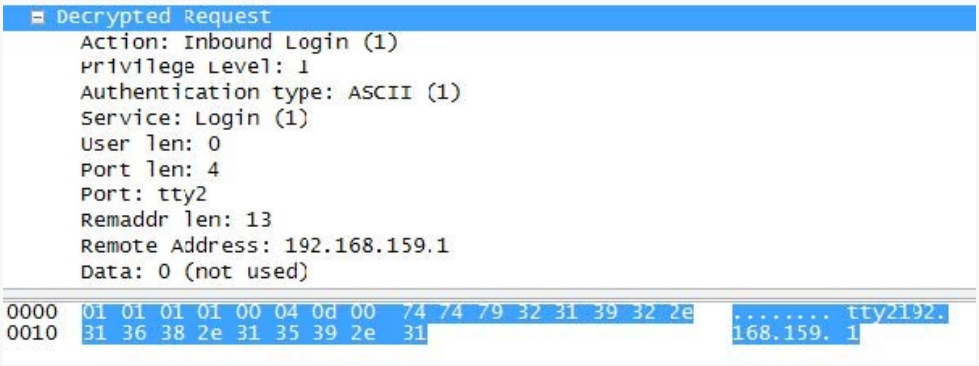

Рис. 2. Результати атаки

Що тут можна побачити? Найголовніше – відсутність по-справжньому випадкових значень. За моїми спостереженнями, змінюються лише Port, RemAddr та RemAddrLen, можливо Priv Level. Але якщо можна провести MITM-атаку на Cisco та TACACS+, то є і можливість підключатися до цього ж Cisco для аутентифікації на ньому (при цьому валідних ключів і не потрібно знати).

У цій ситуації ми вже контролюватимемо частину незашифрованих даних, що передаються від пристрою на TACACS+. Ми знаємо свій IP і досить впевнені в значенні Priv Level (адже ми намагаємося підключитися віддалено). Залишається лише Port. Але й тут значення, найімовірніше, буде tty плюс номер tty. А з урахуванням того, що у Cisco TTY не так багато (зазвичай від 0 до 4) і йдуть вони послідовно (залежно від кількості паралельних сесій), ми приходимо до висновку, що варіантів незашифрованих даних першого пакета за нашої аутентифікації один чи два.

Тепер у нас є зашифровані дані (enc_data), 16 байт незашифрованих початкових даних (data) та повторних. За допомогою XOR ми отримуємо хеш MD5_1 (точніше, декілька – залежно від кількості варіантів незашифрованих даних). Тепер ми можемо згодувати MD5 в oclHashCat і брукувати ключ. У разі успіху ми зможемо розшифрувати з тим самим ключем та автентифікації реальних адмінів Cisco на TACACS+.

Але це ще не все цікаве, що можна отримати з цієї атаки. Якщо ближче придивитися до шифрування протоколу TACACS+, можна помітити, що MD5 використовується поле `seq_no`, тобто номер пакета. Таким чином, для кожного пакета даних буде генеруватися свій `pseudo_pad`, а це означає, що MD5_1 вийде витягти з будь-якого запиту чи відповіді. Це значно полегшує завдання, оскільки можна вибрати пакет даних, у якому точно впевнені.

Зламування роутерів CISCO за допомогою SYNful Knock

SYNful Knock – прихована модифікація прошивки CISCO роутерів, яка може бути використана для підтримки витривалості в мережі жертви [7]. Вона настроюється і модульна, тому може бути оновлена після впровадження. Також присутність бекдора* буде важко детектувати, тому що використовується нестандартні пакети, як при псевдоаутентифікації.

Спосіб ін'єкції полягає в модифікованому образі Cisco IOS, яка дозволяє атакуючому завантажувати різні функціональні модулі із зовнішньої мережі (з інтернету здебільшого). Ін'єкція також надає необмежений доступ до використання секретного пароля від бекдора. Кожен із модулів підключений через HTTP (не HTTPS), використовуваний спеціально складені пакети TCP, що надсилаються на інтерфейс роутерів. Ці пакети мають нестандартну послідовність та відповідні коригувальні числа. Модулі можуть визначати себе, як код, що виконується незалежно, або «гаки» (hooks) для ОС роутерів, які надають функціонал

аналогічно паролям для бекдорів. Ну а пароль для бекдорів надає доступ до роутера через консоль та Telnet.

Відомі на даний момент моделі, схильні до вразливості: *Cisco 1841 router; Cisco 2811 router; Cisco 3825 router*. Інші моделі теж схильні до цієї вразливості, якщо вони засновані на схожій базовій функціональності та на базі коду IOS.

Ін'єкція знаходиться всередині модифікованого образу Cisco IOS, і коли вона вже завантажена (впроваджена), то ін'єкція зберігається в системі, навіть після перезавантаження. Однак подальші модулі, завантажені атакуючим, будуть доступні тільки на час поточного сеансу ОС і вивантажаться з пам'яті після ребута.

Загальний опис алгоритму атаки.

Зміни бінарного коду IOS можуть бути розділені на чотири функції:

1. Модифікувати атрибути читання/запису трансляції асоціативного буфера (translation lookaside buffer – TLB).
2. Модифікувати стандатртну функцію IOS для її подальшого виклику та ініціалізувати ШПЗ.
3. Перезаписати стандартний протокол обробки функцій, що містять шкідливий код.
4. Перезаписати рядки, що належать до стандартних функцій, рядками, що використовуються ШПЗ.

ШПЗ примушує всі атрибути TLB читання або запису ставати атрибутами читання-запису (RW). Ця зміна потрібна для забезпечення можливості «захоплення» (hooking) функцій IOS модулями, що завантажуються. Якщо ж ці атрибути не будуть виставлені як RW, зміни кешованих сторінок можуть не поширитися на оригінальні сторінки в пам'яті. Це досягається шляхом зміни двох одиночних байт функції IOS, яка покликана відповідати за конфігурацію TLB. Незмінена функція встановлює перші два біти регістра в одиницю, і змінена функція встановлює перші три біти на 1.

Модифікація TLB атрибутів:

```
Original:
.text:XXXXXXXX 36 D2 00 03              ori     $s2, $s6, 3
.text:XXXXXXXX 36 91 00 03              ori     $s1, $s4, 3


Modified
.text:XXXXXXXX 36 D2 00 07              ori     $s2, $s6, 7
.text:XXXXXXXX 36 91 00 07              ori     $s1, $s4, 7
```

Залежно від типу роутера, точні діапазони адрес пам'яті зазвичай вказують на секції коду, що виконується, доступні тільки для читання. Найпростіший спосіб визначити, чи було змінено роутер – це використовувати команду `show platform | include RO, Valid`«. Образ IOS міг бути модифікований для можливості зміни коду, що виконується, якщо результати не відображаються.

Для виконання ШПЗ, поки завантажується образ IOS, змінюється функція, що відповідає за планування процесів. Щоб уникнути зміни розмірів образу, ШПЗ перезаписує деякі стандартні функції IOS своїм виконуваним кодом. Атакуючий перевіряє, що перезапис цих функцій не викликає в системі збоїв за певних (потрібних йому) умов. Незважаючи на те, що розмір образа не змінюється, ШПЗ все ж таки перезаписує деякі рядки репорту своєю конфігурацією. Це ще одна ознака того, що образ був модифікований ШПЗ. Нижче наведено стандартні рядки, які мають відображатися при нормальному образі:

```
XXXXXXXX  65 63 20 00 2C 20 43 6F 6E 66 69 67 75 72 65 64  ec ., Configured
XXXXXXXX  20 49 6E 74 65 72 76 61 6C 20 25 64 20 73 65 63   Interval %d sec
XXXXXXXX  00 00 00 00 0A 4E 65 78 74 20 75 70 64 61 74 65  .....Next update
XXXXXXXX  20 64 75 65 20 69 6E 20 00 00 00 00 0A 43 75 72   due in .....Cur
XXXXXXXX  72 65 6E 74 20 74 69 6D 65 20 25 54 61 00 00 00  rent time %Ta...
XXXXXXXX  0A 49 6E 64 65 78 20 25 64 20 54 69 6D 65 73 74  .Index %d Timest
XXXXXXXX  61 6D 70 20 25 54 61 00 0A 0A 46 61 69 6C 75 72  amp %Ta...Failur
XXXXXXXX  65 20 48 65 61 64 20 25 64 2C 20 4C 61 73 74 20  e Head %d, Last
XXXXXXXX  25 64 20 4C 53 41 20 67 72 6F 75 70 20 66 61 69  %d LSA group fai
XXXXXXXX  6C 75 72 65 20 6C 6F 67 67 65 64 00 0A 54 69 6D  lure logged..Tim
```

Ці рядки замінюються на такі (або подібні до наступних):

```
XXXXXXXX  00 00 00 00 00 00 00 00 00 00 00 00 48 54 54 50  ............HTTP
XXXXXXXX  2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 53 65 72  /1.1 200 OK..Ser
XXXXXXXX  76 65 72 3A 20 41 70 61 63 68 65 2F 32 2E 32 2E  ver: Apache/2.2.
XXXXXXXX  31 37 20 28 55 62 75 6E 74 75 29 0D 0A 58 2D 50  17 (Ubuntu)..X-P
XXXXXXXX  6F 77 65 72 65 64 2D 42 79 3A 20 50 48 50 2F 35  owered-By: PHP/5
XXXXXXXX  2E 33 2E 35 2D 31 75 62 75 6E 74 75 37 2E 37 0D  .3.5-1ubuntu7.7.
XXXXXXXX  0A 4B 65 65 70 2D 41 6C 69 76 65 3A 20 74 69 6D  .Keep-Alive: tim
XXXXXXXX  65 6F 75 74 3D 31 35 2C 20 6D 61 78 3D 31 30 30  eout=15, max=100
XXXXXXXX  0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65  ..Connection: Ke
XXXXXXXX  65 70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E  ep-Alive..Conten
```

Пароль бекдору. Атакуючий може використовувати секретний пароль бекдору у трьох різних ситуаціях. Ін'єкція спочатку перевіряє, чи є введені користувачем дані паролем від бекдора. Якщо ні, то впроваджується код, який передаватиме параметри доступу при верифікації. Наступні три приклади були перевірені на можливість отримання доступу, використовуючи пароль бекдору (табл. 1).

Таблиця 1

Результати перевірки на отримання доступу

Метод	Підказка	Результат
Console	User Access Verification	Access and elevated session
Telnet	Username is the backdoor password	Access and elevated session
Elevation (enable)	Enable password	Elevated session

Дослідження показало, що HTTPS та SSH не можуть бути використані для цих цілей.

Управління ін'єкцією. Керуюча частина ін'єкції також є модульною і дозволяє підвантажувати додатковий функціонал в IOS. Фукціональність управління непомітна, тому що запитує серії TCP пакетів, які ШПЗ моніторить на наявність спеціальних значень у заголовку та контенті.

1. Для початку процесу, унікально складений TCP SYN пакет відправляється на 80 порт зараженого роутера. Важливо уточнити, що різниця між числом у полі Sequence і acknowledgment має бути встановлена значення `0xC123D`.

2. Як і ШПЗ відповідає триетапними SYN-ACK повідомленнями підтверджуючи перше SYN повідомлення. Однак можна помітити такі умови, що дотримуються:

різниця між полями acknowledgment та sequence – `0xc123e`;

наступні жорстко закодовані TCP опції встановлюються: "`02 04 05 b4 01 01 04 02 01 03 03 05`";

необхідний вказівник виставлено на значення `0x0001`, але необхідний прапор не встановлюється;

ШПЗ копіює acknowledgment number з SYN пакета для sequence number. Хоча зазвичай сервер генерує рандомний sequence number, тому це стандартний хендшейк TCP.

3. Після кінцевого ACK'а для завершення триетапного хендшейка контролер відправляє наступне TCP-повідомлення:

PUSH та ACK прапори встановлені;

від початку заголовка TCP на зміщенні `0x62` вписується рядок «text»;

команда, наведена нижче, встановлюється на зсуві `0x67` щодо заголовка TCP:

```
[4 byte Command Length][CMD Data][4 byte checksum]
```

4. Відповідь ШПЗ інкапсулюється в наступній статичній HTTP/HTML відповіді сервера:

```
HTTP/1.1 200 OK
Server: Apache/2.2.17 (Ubuntu)
X-Powered-By: PHP/5.3.5-1ubuntu7.7
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
<html><body><div>[Response]</div></body></html>
```

Висновки

У даній статті було проведено дослідження потенційних уразливостей роутерів Cisco до зовнішніх ін'єкцій. Дослідження виявило, що роутери Cisco, незважаючи на свою популярність та надійність, можуть бути піддані різноманітним загрозам, пов'язаним з ін'єкціями шкідливого коду або даних. Результати дослідження підкреслюють необхідність постійного моніторингу та підвищення безпеки мереж, які використовують роутери Cisco. Зовнішні ін'єкції можуть призвести до серйозних наслідків, включаючи втрату конфіденційності даних, порушення цілісності та доступність мережевих ресурсів. Рекомендації для користувачів роутерів Cisco включають у себе зміну стандартних паролів, регулярне оновлення програмного забезпечення та налаштування брандмауера для обмеження доступу до критичних ресурсів. Крім того, важливо підвищувати свідомість щодо кібербезпеки та навчатися відповідним методам і практикам.

Загальний висновок полягає в тому, що забезпечення безпеки мережевого обладнання, зокрема роутерів Cisco, є критично важливим завданням у сучасному світі. Дослідження та практичні рекомендації, надані в цій статті, можуть слугувати як основа для подальших заходів забезпечення безпеки та захисту від зовнішніх ін'єкцій у мережах, що використовують роутери Cisco.

Перелік посилань

1. Clausen, T. H. & Herberg, U. (2010). Vulnerability Analysis of the Optimized Link State Routing Protocol version 2 (OLSRv2). 10.1109/WCINS.2010.5544732.

2. Jeitner, P., Shulman, H., Teichmann, L., Waidner M. XDRI Attacks - and - How to Enhance Resilience of Residential Routers. 31th USENIX Security Symposium (USENIX Security 22), 2022

3. Rotenberg, N., Shulman, H., Waidner, M., and Zeltser B. 2017. Authentication-Bypass Vulnerabilities in SOHO Routers. In Proceedings of SIGCOMM Posters and Demos '17, Los Angeles, CA, USA, August 22–24, 2017, 3 pages. https://doi.org/10.1145/3123878.3131989

4. Wang, F., & Wu, S. F. (1998). On the vulnerabilities and protection of OSPF routing protocol. Proceedings 7th International Conference on Computer Communications and Networks (Cat. No.98EX226), 148-152.

5. AlRubaiei, M., Jassim, H. sh, Baraa, T. Sharef, S. S., Sharef, Z. T., Malallah F. L. 6 - Current vulnerabilities, challenges and attacks on routing protocols for mobile ad hoc network: a review, In Intelligent Data-Centric Systems, Swarm Intelligence for Resource Management in Internet of Things, Academic Press, 2020, Pages 109-129, ISBN 9780128182871, https://doi.org/10.1016/B978-0-12-818287-1.00012-7.

6. Matveev, D. Taming CISCO - brute force the key to TACACS+. https://cryptoworld.su

7. Matveev, D. Hacking CISCO routers using SYNful Knock https://cryptoworld.su.

Надійшла 14.03.2024