**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**---------------------**



**BÁO CÁO CHUYÊN ĐỀ**

**TỐT NGHIỆP**

**Đề tài:**

**PHÂN TÍCH VÀ XÂY DỰNG CHƯƠNG TRÌNH PHÁT HIỆN CVE-2018-16858**

**Giáo viên hướng dẫn : ThS. PHAN NGHĨA HIỆP**

**Sinh viên thực hiện : NGUYỄN VĂN THANH TÚ**

**Mã số sinh viên : N18DCAT077**

**Lớp : D18CQAT01-N**

**Khóa : 2018 – 2023**

**Hệ : ĐẠI HỌC CHÍNH QUY**

**Tp.Hồ Chí Minh, tháng 11 năm 2022**

1. TÌM HIỂU VỀ LIBREOFFICE
   1. Thông tin Libre Office

LibreOffice là bộ ứng dụng văn phòng mã nguồn mở do The Document Foundation phát triển. Nó phân nhánh từ OpenOffice.org năm 2010, phiên bản nguồn mở của StarOffice trước đó. Bộ LibreOffice bao gồm trình xử lý văn bản, ứng dụng bảng tính, trình chiếu, sơ đồ và bản vẽ, làm việc với cơ sở dữ liệu và soạn thảo công thức toán học. Nó có sẵn trong 115 ngôn ngữ. Mục tiêu của các lập trình viên khi phát triển nó là tạo ra một bộ phần mềm văn phòng không phụ thuộc vào nhà cung cấp nào, có hỗ trợ ODF và không đòi hỏi phải có sự chuyển nhượng bản quyền nào. Tên phần mềm là một từ ghép giữa Libre, có nghĩa là tự do trong tiếng Tây Ban Nha và tiếng Pháp, cùng với từ Office (văn phòng) của tiếng Anh. LibreOffice sử dụng định dạng file OpenDocument (ODF) theo chuẩn ISO/IEC OpenDocument làm định dạng chính để lưu các tài liệu cho tất cả các ứng dụng của nó. LibreOffice cũng hỗ trợ các định dạng file của hầu hết các bộ văn phòng lớn khác, bao gồm Microsoft Office, thông qua nhiều bộ lọc nhập/xuất. LibreOffice có sẵn cho nhiều nền tảng máy tính khác nhau, bao gồm Microsoft Windows, macOS, Linux, Android,iOS, và Chromebook. Cũng như dưới dạng một bộ văn phòng trực tuyến LibreOffice Online. Nó là bộ ứng dụng văn phòng mặc định của hầu hết các bản phân phối Linux phổ biến. Đây là bộ phần mềm văn phòng tự do nguồn mở được phát triển tích cực nhất, với hoạt động phát triển gấp khoảng 50 lần Apache OpenOffice, hậu duệ lớn khác của OpenOffice.org. Dự án đã được công bố và bản beta được phát hành ngày 28 tháng 9 năm 2010. Từ tháng 1 năm 2011 (bản phát hành chính thức đầu tiên) và tháng 10/2011, LibreOffice đã được tải xuống khoảng 7,5 triệu lần. Dự án tuyên bố 120 triệu địa chỉ tải xuống duy nhất từ tháng 5/2011 đến tháng 5/2015, không bao gồm các bản phân phối Linux, với 55 triệu trong số đó là từ tháng 5/2014 đến tháng 5/2015.

* 1. Hệ điều hành

Các nhà phát triển The Document Foundation hướng mục tiêu của LibreOffice đến Microsoft Windows (IA-32 và x86-64), Linux (IA-32, x86-64 và ARM) và macOS (x86-64). Đồng ports đến FreeBSD, NetBSD, OpenBSD và Mac OS X 10.5, PowerPC nhận được hỗ trợ từ những người đóng góp cho những dự án, tương ứng LibreOffice cũng được cài trên OpenIndiana thông qua SFE.

Các phiên bản tiền nhiệm trong lịch sử của LibreOffice, trở lại StarOffice 3, đã chạy trên Solaris với các CPU SPARC mà Sun Microsystems (và sau này là Oracle) sản xuất. Bản port không chính thức của LibreOffice, các phiên bản hiện đã lỗi thời, đã hỗ trợ SPARC. Các port không chính thức hiện LibreOffice 5.2.5 chỉ chạy trên phần cứng tương thích với Intel, cho đến Solaris 11.

Năm 2011, các nhà phát triển đã công bố kế hoạch port LibreOffice sang Android và iOS. Phiên bản beta của trình xem tài liệu cho Android 4.0 trở lên đã được phát hành vào tháng 1 nặm 2015; Tháng 5/2015, LibreOffice Viewer for Android đã được phát hành với khả năng chỉnh sửa cơ bản.

1. TÌM HIỂU CVE-2018-16858
   1. Thông tin phiên bản LibreOfice chứa CVE-2018-16858

LibreOffice có một tính năng cho phép các tài liệu có thể chỉ định rằng các macro được cài đặt sẵn có thể được thực thi trên các sự kiện khác nhau như chuyển đổi chuột, v.v.

Các phiên bản LibreOffice trước 6.0.7/6.1.3 dễ bị tấn công bằng thư mục trong đó có thể tạo một tài liệu mà khi LibreOffice mở ra, sẽ thực hiện phương thức Python từ một tập lệnh ở bất kỳ vị trí hệ thống tệp tùy ý nào, được chỉ định liên quan đến vị trí cài đặt LibreOffice.

Thông thường LibreOffice được gói với Python, vì vậy một kẻ tấn công có một tập hợp các tập lệnh đã biết tại một vị trí hệ thống tệp tương đối đã biết để làm việc. Trong phiên bản 6.1, vấn đề này được kết hợp bởi một tính năng bổ sung cho phép chỉ định trong các đối số tài liệu chuyển sang phương thức Python (chuỗi trước đó chỉ cho phép một phương thức được gọi mà không có đối số). Python đi kèm xảy ra bao gồm một phương thức thực thi thông qua hệ điều hành.

1. XÂY DỰNG CHƯƠNG TRÌNH PHÁT HIỆN CVE-2018-16858
   1. Thiết lập môi trường
      1. Máy nạn nhân (victim)

Máy Window 10 đóng vai trò là máy nạn nhân có địa chỉ IP là 172.16.1.6 cài đặt phiên bản Libreoffice 6.1.2.1

Text

Description automatically generated

**Hình 3.1 Địa chỉ IP máy nạn nhân**

Graphical user interface, application

Description automatically generated

**Hình 3.2 Phiên bản LibreOffice 6.1.2.1 được cái trên máy nạn nhân**

* + 1. Máy tấn công (attacker)

Máy Kali Linux có IP là 172.16.1.12 lưu trữ file odt chứa CVE-2018-16858 và là máy lắng nghe RCE.

Text

Description automatically generated

**Hình 3.3 Địa chỉ IP máy tấn công**

* 1. Thực hiện tấn công

Trên máy attacker sử dụng metasploit, Libre Office Macro Reception cung cấp một tệp ODT và chỉ định lhost, lport và payload sẽ được nhúng vào.

Text

Description automatically generated

**Hình 3.4 Tạo file odt chứa mã độc bằng metasploit**

Tệp đã được nhúng sẽ lưu trong đường dẫn /root/.msf4/local/ với tên tệp là librefile.odt. Tiến hành dùng http.server đẩy thư mục chứa file mã độc lên port 3456.

Text

Description automatically generated

Trên máy nạn nhân truy cập vào url 172.16.1.12:3456 để download file odt về máy.

Graphical user interface, application

Description automatically generated

**Hình 3.5 truy cập vào url 172.16.1.12:3456 để download file odt**

Tiếp theo mở tệp odt trên máy victim sẽ xảy ra lỗi đọc/ghi.

Graphical user interface, application, Word

Description automatically generated

**Hình 3.6 Mở file odt vừa download**

Trên máy attacker bắt đầu handler

Text

Description automatically generated

**Hình 3.7 Thực hiện quá trinh handler trên máy tấn công**

* 1. Thu thập dữ liệu

Quá trình tấn công được thu thập lại thông qua Wireshark. Dữ liệu thu thập được khi download file odt chứa mã độc từ máy tấn công về máy nạn nhân.

Text

Description automatically generated

**Hình 3.8 Gói tin khi download file odt chứa mã độc**

Dữ liệu thu thập được sau khi mở tệp librefile.odt trên máy victim và trên máy attacker bắt đầu handler.

Graphical user interface, text, application

Description automatically generated

**Hình 3.9 Các gói tin trong quá trình RCE**

* 1. Phân tích

LibreOffice đi kèm với các macro mẫu được viết bằng Python và cho phép khả năng liên kết các sự kiện chương trình với họ. Một macro có thể được gắn với một sự kiện chương trình bằng cách bao gồm tập lệnh chứa macro và tên hàm sẽ được thực thi. Ngoài ra, một lỗ hổng truyền tải thư mục tồn tại trong thành phần tham chiếu tập lệnh Python sẽ được thực thi. Điều này cho phép một sự kiện chương trình thực hiện các chức năng từ các tập lệnh Python so với đường dẫn của thư mục Macros mẫu. Tập lệnh pydoc.py trong libreoffice chứa hàm tempfilepager chuyển các đối số cho hệ điều hành và cho phép RCE.

Các Python scripts được đóng gói với Libre Office cũng có thể được truy cập từ các scripts này thông qua một lỗ hổng truyền tải tệp. Cái dễ bị tổn thương được sử dụng là OC.PY có thể được truy cập thông qua lỗ hổng truyền tải tệp bằng cách thay thế một phần của văn bản trong content.xml.

xlink:href=”vnd.sun.star.script:../../../program/python-core-3.5.5/lib/pydoc.py$tempfilepager(1,<payload>)?language=Python&amp;location=share” xlink:type=”simple”

Trong cuộc tấn công trên ta phát hiện payload được nhúng vào trong script của content.xml

Text

Description automatically generated

**Hình 3.10 Gói tin chứa file odt khi download**

Signature của CVE-2018-16858: **../program/python-core-3.5.5/lib/pydoc.py$tempfilepager**

* 1. Xây dựng công cụ phát hiện CVE-2018-16858

Sử dụng tcpdump bắt real-time các gói và đọc vào stdout



**Hình 3.11 Sử dụng tcpdump bắt gói và đọc ra stdout**

Thực hiện decode stdout thu được và kiểm tra có Signature CVE-2018-16858



**Hình 3.12 Signature của CVE-2018-16858**

A screenshot of a computer

Description automatically generated with medium confidence

**Hình 3.13 Kiểm tra signature trong gói tin**

Ghi tất cả các gói tin bắt được vào file txt.

Chạy chương trình phát hiện CVE-2018-16858



**Hình 3.14 Chạy code phát hiện CVE-2018-16858 với interface cần bắt gói**

Chương trình cho kết quả có CVE-2018-16858 trong traffic và cho biết thông tin về địa chỉ IP và Port từ máy chứa odt mã độc.

Text

Description automatically generated

**Hình 3.15 Phát hiện CVE-2018-16858 trong traffic**