Cảnh báo lỗ hổng 0-day cho phép thực thi mã tùy ý trên Microsoft Windows với tên gọi là Follina. Lỗ hổng hiện đã được gán nhãn CVE-2022-30190, cho phép thực thi mã tùy ý qua Microsoft Office kể cả khi đã tắt Macro. Đặc biệt khi tệp tin ở định dạng RTF thì mã sẽ được thực thi mà không cần người dùng mở tệp cũng như sẽ tự động bypass tính năng Protected View trong MS Office.

Phạm vi ảnh hưởng/Điều kiện khai thác:

• Sử dụng một trong các phiên bản Windows sau:

o Windows Server 2012 R2 (Server Core installation)

o Windows Server 2012 R2

o Windows Server 2012 (Server Core installation)

o Windows Server 2012

o Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server

Core installation)

o Windows Server 2008 R2 for x64-based Systems Service Pack 1

o Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

o Windows Server 2008 for x64-based Systems Service Pack 2

o Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

o Windows Server 2008 for 32-bit Systems Service Pack 2

o Windows RT 8.1

o Windows 8.1 for x64-based systems

o Windows 8.1 for 32-bit systems

o Windows 7 for x64-based Systems Service Pack 1

o Windows 7 for 32-bit Systems Service Pack 1

o Windows Server 2016 (Server Core installation)

o Windows Server 2016

o Windows 10 Version 1607 for x64-based Systems

o Windows 10 Version 1607 for 32-bit Systems

o Windows 10 for x64-based Systems

o Windows 10 for 32-bit Systems

o Windows 10 Version 21H2 for x64-based Systems

o Windows 10 Version 21H2 for ARM64-based Systems

o Windows 10 Version 21H2 for 32-bit Systems

o Windows 11 for ARM64-based Systems

o Windows 11 for x64-based Systems

o Windows Server, version 20H2 (Server Core Installation)

o Windows 10 Version 20H2 for ARM64-based Systems

o Windows 10 Version 20H2 for 32-bit Systems

o Windows 10 Version 20H2 for x64-based Systems

o Windows Server 2022 Azure Edition Core Hotpatch

o Windows Server 2022 (Server Core installation)

o Windows Server 2022

o Windows 10 Version 21H1 for 32-bit Systems

o Windows 10 Version 21H1 for ARM64-based Systems

o Windows 10 Version 21H1 for x64-based Systems

o Windows Server 2019 (Server Core installation)

o Windows Server 2019

o Windows 10 Version 1809 for ARM64-based Systems

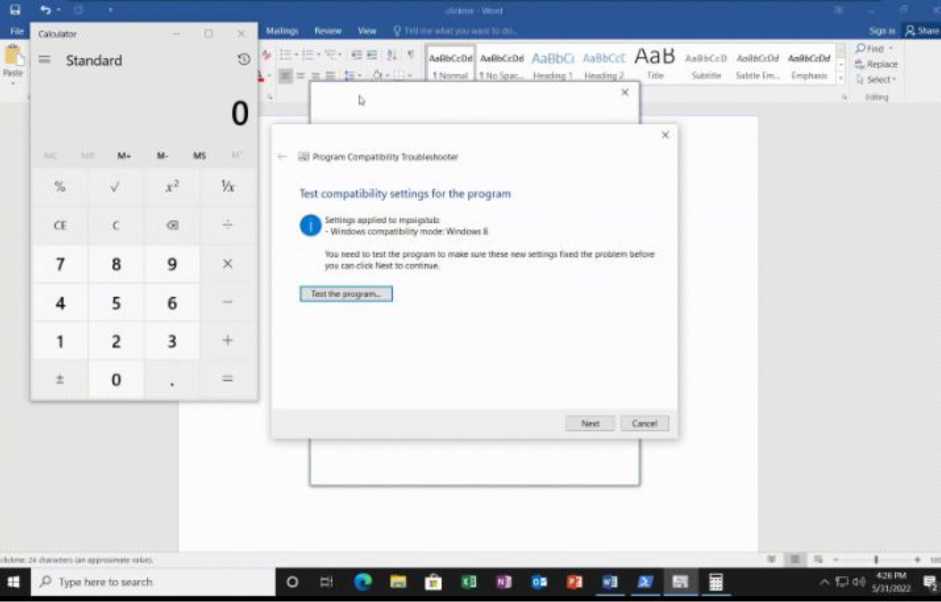
o Windows 10 Version 1809 for x64-based Systems

o Windows 10 Version 1809 for 32-bit Systems

• Ngoài ra tin tặc cần lừa người dùng tải về file độc hại

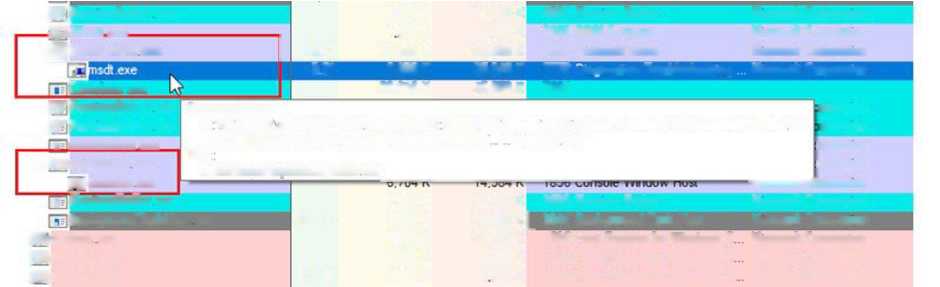
Thông tin chi tiết:

Lỗ hổng xảy ra khi Microsoft Support Diagnostic Tool (**MSDT**-đây là công cụ chuẩn đoán lỗi mặc định của Microsoft) được gọi bằng giao thức URL từ ứng dụng (ví dụ như Word) kết hợp với một phần lỗi trong bộ xử lý HTML của Microsoft sẽ làm thực thi payload trong đó ( < 4096 byte )

Lỗ hổng cho phép thực thi mã tùy ý qua Microsoft Office kể cả khi đã tắt Macro. Nếu tệp tin ở định dạng RTF thì mã sẽ được thực thi mà không cần người dùng mở tệp cũng như bypass tính năng Protected View trong MS Office.

Dấu hiệu tấn công/nhận biết:

Tính năng MSDT rất ít được sử dụng đặc biệt khi sinh ra từ tiến trình cha gọi từ các ứng dụng như Winword ví dụ như sau:



I < 0.01

Caicdator exe

23.916 K

Command Line:

irporation

"C ''Windows system32Mnsdt exe" ms-msdt /id PCWDiagnostic /skip force /param ~IT\_RebrowseForFile=‘> IT rporation

5.376 K

3,212 K

9.992 K

2,408 K

1.532 K

31.380K

7.440 K

190.896 K

9.016 K

1 508 K

97.100 K

14.412 K

3.720 K

1 896 K

896 Host Process for Windows s Microsoft Corporation

944 Host Process for Windows s Microsoft Corporation

824 Host Process for Windows s. Microsoft Corporation

22.168K 1808 Runhme Broker

16.432 K| 3644 Background Task Host

-LaunchMethod =ContextMenu IT\_BrowseForFile=/.7 /S(caỉc)/ exe” Path

C:\Wmdow8\System32\msdt exe

. backgroundTaskHost exe

[TjSvchost exe

IT svchost.exe

rTsvchost.exe

45.076 K 7164

irporation irporation

THTCrororr-corporation

Microsoft Corporation

Microsoft Corporation

[T Runtime Broker exe IT ỆBỊnÍỄme Broker exe . smartscreen exe

□ T sdiagnhost exe

part conhost exe

I Runtine Broker exe

FT] jfrfrne Broker exe ■T.dfcnst are

0(3 WINWORD EXE

Susp...

<0.01

6.852 K

<0 01

| 4204 Rurtme Broker | Microsoft Corporation |
| --- | --- |
| 8180 COM Surrogate  4092 Microsoft Word | Microsoft Corporation  Microsoft Corporation |

25.848 K 3772 WMoostes Troubleshooting Microsoft Coiporation

**Cách phòng tránh/fix lỗi/phát hiện:**

1. Lỗ hổng chưa có dấu hiệu nhận biết cụ thể khác và chưa có bản vá từ phía hãng.
2. Cách khắc phục tạm thời: Tắt giao thức MSDT URL (tham khảo: [https://msrc-](https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/) blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft- support-diagnostic-tool-vulnerability/[)](https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/) hoặc làm như sau:

* Chạy CMD với quyền admin.
* Chạy lệnh "reg export HKEY\_CLASSES\_ROOT\ms-msdt filename" để lưu lại register key.
* Chạy lệnh "reg delete HKEY\_CLASSES\_ROOT\ms-msdt /f"

1. Ngoài ra có thể tham khảo rule phát hiện tại:

<https://github.com/GossiTheDog/ThreatHunting/blob/master/AdvancedHunting> Queries/Follina-Office. ahq