ICT379: Project Vulnerability Detection and Mitigation Report

Vulnerability: Follina (CVE2022-30190)

Submission Date:

Group Name: FTB-02

Students: Yin Zhangpeng (34742217) and Lucas Goh (34747611)

Table of Contents

Introduction

This report examines CVE-2022-30190, also known as "Follina," a critical Remote Code Execution (RCE) vulnerability within the Microsoft Windows Support Diagnostic Tool (MSDT). Discovered in May 2022, Follina poses significant risks to users and organizations by allowing malicious actors to execute arbitrary commands on affected systems. This report aims to comprehensively understand vulnerability, its potential impact, and effective mitigation and detection strategies.

The first part of this report provides a detailed overview of how the Follina vulnerability operates, including the technical mechanisms behind its exploitation. It also outlines our proposed test environment for demonstrating mitigation and detection techniques. The subsequent sections detail how to detect the Follina exploitation using Process Explorer, a system monitoring tool. Lastly, the report will discuss various implementations to mitigate the exploit, such as disabling MSDT URL Protocol through the Windows Registry or deploying an intrusion prevention system such as Snort to drop packets that exhibit the Follina exploitation behaviour and characteristics.

Vulnerability Description and Exploitation

CVE-2022-30190, commonly known as Follina, is a remote code execution vulnerability within the Microsoft Windows Support Diagnostic Tool (MSDT). This vulnerability exploits a flaw in how MSDT processes malformed URIs, leading to a read only buffer overflow that allows for arbitrary command execution.

Vulnerability Outcomes

The systems affected by CVE-2022-30190 (Follina) include various Windows operating systems where Microsoft Office is installed. Specifically, the vulnerability impacts:

- Windows Server 2022/2019/2016/2012 & 2012 R2/2008 R2
- Windows 11/10/8.1
- Windows 7 Service Pack 1

The core mechanism of this exploit involves using a customized Word document containing a malicious URL. This URL points to a webpage with HTML text padded to reach a buffer size of 4096 bytes, followed by a JavaScript payload that invokes the ms-msdt protocol handler. When the Word document is opened or previewed, it attempts to load the external HTML file, which then triggers MSDT via the ms-msdt: URL schema.

Attackers can exploit this vulnerability by crafting these URLs with embedded PowerShell commands or other malicious scripts. These commands, when executed, perform unauthorized actions on the victim's system, such as downloading and running malware or altering system configurations. The exploit executes based on the user’s privileges, leading to remote code execution, which may lead to other attacking vectors such as privilege escalation or theft of sensitive data information.

Exploit history and discovery

The Follina vulnerability, also known as CVE-2022-30190, was discovered in May 2022 and has been actively exploited by threat actors. Microsoft issued security updates for the affected products in June 2022, but many systems remain unpatched and vulnerable. The timeline of Follina reveals significant events: a bachelor thesis explaining the use of MSDT for code execution was released in August 2020, and researchers reported the use of Microsoft Office URIs for code execution to Microsoft in March 2021. On April 12, 2022, a report on observed exploitation was submitted to Microsoft MSRC, but the ticket was closed on April 21, 2022, as it was not considered a security-related issue. However, the execution of MSDT with macros disabled was recognized as a concern.

Follina gained public attention on May 27, 2022, when it was disclosed in a tweet by @nas_sec. Microsoft assigned the CVE identifier CVE-2022-30190 on May 30, 2022, and activated Defender antivirus and EDR signatures. The earliest documented instance of malware using Follina was observed on April 7, 2022. Microsoft categorized it as a zero-day vulnerability on May 31, 2022, and a CISA advisory was released. A patch for the vulnerability was included in the June 14, 2022, Patch Tuesday releases.

Vulnerability Mechanism

The core mechanism for this exploit involves using a customized Word document with a malicious URL. The URL leads to a webpage containing HTML text with random letters until it reaches the 4096 bytes buffer size, followed by the JavaScript payload that invokes the ms-msdt handler.

The Attack Process is as such:

1. **Initial Vector**: A malicious Microsoft Word document is created containing a link to an external HTML file.
2. **Document Structure**: The document includes a document.xml.rels file pointing to a remote URL hosting the malicious HTML. As shown in Figure A2 of the appendix, Hammond (n.d.).
3. **HTML Payload**: The HTML file contains a script with many padding characters and a PowerShell command. As shown in Figure A3 of the appendix, Hammond (n.d.).
4. **Triggering the Exploit**: When the Word document is opened or even previewed, it attempts to load the external HTML file. The HTML file triggers the Microsoft Support Diagnostic Tool (MSDT) via the ms-msdt: URL schema.
5. **Execution**: The PowerShell command embedded in the URL is executed. The command decodes a Base64 encoded string and executes it to run cmd.exe, which runs several commands to download and execute additional payloads.
6. **Malware Deployment**: The payload is a RAR file containing an encoded CAB file. The CAB file is decoded and expanded, and a final executable (rgb.exe) is run, delivering the actual malware.

Refer to Figure A1 of the appendix for a simplified diagram of how the exploit works.

Test Environment for Exploitation

To simulate the Follina vulnerability, we will create a test environment with two virtual machines under the same NAT network for easy communication: one Kali Linux machine and one Windows 10 machine with an older version of Office installed. On the attacker machine, we will run a Python script to create the malicious Word document and host the payload HTML on a web server.

The test involves the victim accessing the web server, downloading the malicious Word document, and opening it. If the exploitation is successful, the attacker will receive a reverse shell from the victim, leading to remote code execution.

Vulnerability Detection

In this scenario, we assume that the Windows Server was initially unprotected against the Follina vulnerability. This means neither the operating system was updated to the latest security patch nor were any modifications applied to the Windows Registry Editor. Since Follina is a remote code execution (RCE) attack, it can penetrate Windows machines if they are connected to the internet. To detect such an attack, we will focus on identifying the types of processes executed when the attack is initiated.

SIEM Solution

The Follina MSDT vulnerability in Microsoft Office can be detected through several methods. Security researchers have developed specific indicators of compromise (IOCs) to identify this exploit, such as monitoring for suspicious processes like "msdt.exe" being launched unexpectedly, particularly by Office applications like Word or Excel. Network security tools can also be configured to detect unusual traffic patterns indicative of exploitation attempts.

SIEM Implementation Using Process Explorer

Process Explorer, a powerful system monitoring tool, can provide detailed information about processes running on a system. To set up detection using Process Explorer, follow these steps:

1. Run Process Explorer: Launch Process Explorer with administrative privileges to ensure it can access all necessary system processes.
2. Monitor for Suspicious Processes: Look for unusual instances of "msdt.exe" being launched, especially by Office applications such as Word or Excel. Normally, "msdt.exe" (Microsoft Support Diagnostic Tool) should not be triggered by these applications, and its appearance can indicate a potential exploitation attempt.
3. Set Up Filters and Alerts: In Process Explorer, set up filters to automatically highlight or alert you to processes that match certain criteria, such as the

execution of "msdt.exe" or any unexpected child processes spawned by Office applications.

4. Analyze Process Details: Use Process Explorer to drill down into the properties of suspicious processes. Check the command line arguments and parent processes to understand better how "msdt.exe" was invoked and to identify any associated malicious activities.

Vulnerability Mitigation

There are many different implementations that can be taken to mitigate the Follina exploit and safeguard the system. The recommended and easiest way of mitigating the exploit would be to update to Microsoft's June 2022 security update. In the event that updating to the June 2022 security update or later is not plausible, several alternatives are shown below.

Disable MSDT URL Protocol

Microsoft has provided a workaround for those unable to update to the necessary security updates by disabling the MSDT URL Protocol through Windows Registry (Msrc, 2022). Disabling the MSDT URL Protocol prevents the Follina exploit as it prevents troubleshooters from launching URL links. The steps taken to disable MSDT URL Protocol on the Windows system provided by Microsoft are detailed below (Msrc, 2022):

1. Open Command Prompt as Administrator.
2. Back up the MSDT registry key with the command:

   reg export HKEYCLASSES_ROOT\ms-msdt _filename
3. Delete the corresponding MSDT registry key with the following command:
   reg delete HKEY_CLASSES_ROOT\ms-msdt /f

Intrusion Prevention System

As disabling the MSDT URL Protocol requires the administrator to delete the MSDT registry keys on the respective computer, it may not be feasible to engage in this arrangement in an enterprise network system. Instead, deploying an intrusion prevention system may be a better solution to safeguard the enterprise network from the Follina exploit by blocking the packets that contain the exploit.

Before applying rules for the intrusion prevention system, we will look at the exploit's characteristics to apply the right rules to mitigate. The characteristics of the exploits according to Kumar & Shah (2022) are:

- External reference to the malicious HTML file with "!" at the end of the reference.
- HTML file containing scripts with a size of over 4096 Bytes for it to be processed.
- Base64 Encoded PowerShell script.
- Windows Event ID 4688 is generated with word application (winword.exe) having a child process of msdt.exe.

With the following characteristics observed from the exploit packets, rules can be implemented to the intrusion prevention system to detect these characteristics and block off

packets that have these characteristics. Snort, an open-source intrusion prevention system will be used to prevent the exploitation. The following rules by Bhdresh (n.d.) will be added to Snort to detect and drop the packet:

drop tcp any any -> any any (msg: "Microsoft Office RCE Exploitation Attempt - Follina"; sid:10020;
flow:from_server,established;content:"HTTP";nocase;offset:0;depth:4;content:"location.href";nocase;distance:0;content:"ms-msdt";nocase;distance:0;content:"PCWDiagnostic";nocase;distance:0;
content:"IT_BrowseForFile";nocase;distance:0;reference:url,
https://github.com/JohnHammond/msdt-follina/blob/main/follina.py; rev:1;)

Applying these rules into Snort should prevent the Follina exploitation from working as it would successfully drop off any packets that show the traits of the exploitation packet.

References

Bhdresh. (n.d.). *SnortRules/Exploit/Follina.rules at master · bhdresh/SnortRules*. GitHub. https://github.com/bhdresh/SnortRules/blob/master/Exploit/Follina.rules

Hammond, J. (n.d.). *Rapid response: Microsoft Office RCE - "Follina" MSDT Attack | Huntress*. https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug

Kumar, V., & Shah, C. (2022, July 19). *Countering follina (MS support diagnostic tool vulnerability : CVE-2022 -30190) attack with Network Security Platform's advanced detection features. Countering Follina (MS Support Diagnostic Tool Vulnerability : CVE-2022 -30190) Attack with Network Security Platform's Advanced Detection Features.* https://www.trellix.com/en-sg/blogs/research/countering-follina-attack-with-network-security-platforms-advanced-detection-features/

Msrc. (2022, May 30). *Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability | MSRC Blog | Microsoft Security Response Center*. https://msrc.microsoft.com/blog/2022/05/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Appendix

Figure A1, Diagram of exploit process

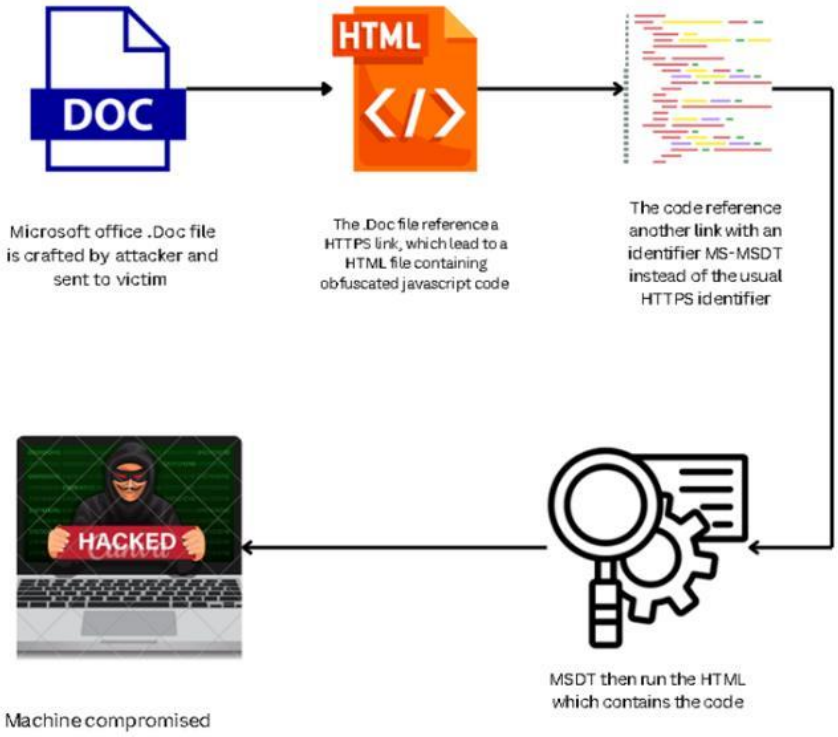
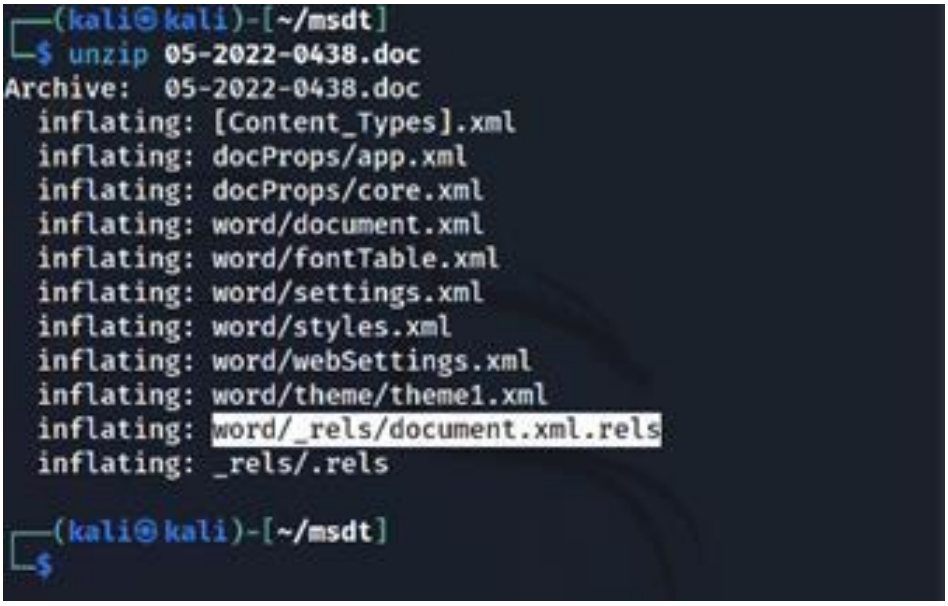
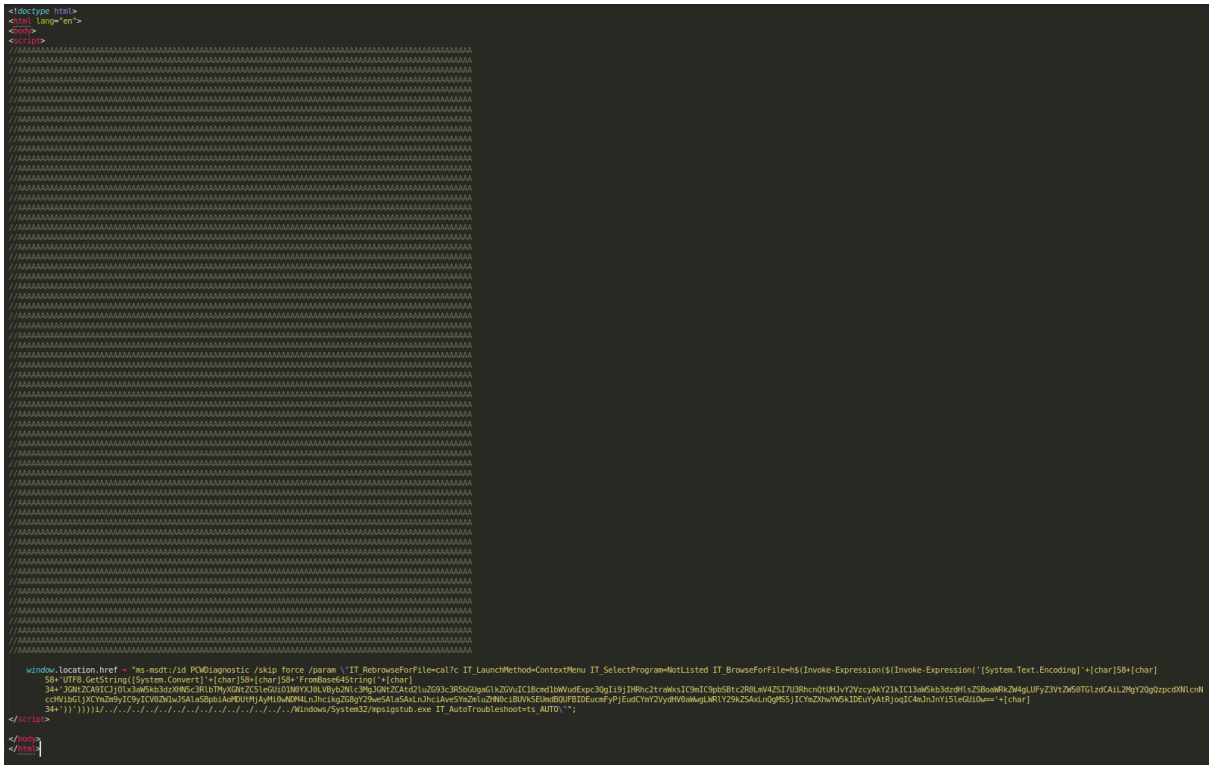


Figure A2, Image of components in the Word document



Note. Gotten from Hammond (n.d.).

Figure A3, Image of the HTML file



Note. Gotten from Hammond (n.d.).