KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

Summary

In the end of May 2022, Independent security researchers identified a vulnerability, CVE-2022-30190, in Microsoft Support Diagnostic Tool (MSDT), which could be exploited to execute arbitrary code when MSDT is accessed using the URI protocol. The URI protocol “ms-msdt:/” could potentially be invoked from the customized word document, allowing malicious code to run on the target machine with the privileges of the calling application. The flaw is dubbed "Follina," and can even execute PowerShell commands over the MSDT. Previously, this vulnerability could circumvent all security measures, including Microsoft Office's Protected View, and run PowerShell scripts just by opening a Word document.

Soon after, threat actors began using it in broad phishing attempts that transmitted QBot and the Rozena backdoor and targeted US government agencies, Ukrainian media organizations, several enterprises, and individuals globally. Microsoft issued a warning and instructions for disabling the MSDT URI protocol in response to the identified vulnerability. The flaw was addressed in Microsoft's June security releases. Since, then this vulnerability has been confirmed to be exploited by several state actors in targeted assault campaigns.

Cyber Threat Analysis

Nomenclature: CVE-2022-30190 - Windows MSDT Follina
Sophistication: Low
Intended Effect: Arbitrary Remote Code Execution on Microsoft Windows
Target: MS Office 2013, 2016, Office Pro Plus and Office 2021
Method: Phishing

Vulnerability Overview

A security researcher discovered the innovative approach while hunting for files that abused CVE-2021-40444 on VirusTotal. He identified a file that exploits the “ms-msdt” scheme by loading HTML via Word's external link, which then leverages the “ms-msdt” scheme to run PowerShell code. This Microsoft Office vulnerability is still being exploited in attempts to execute malicious PowerShell commands via the Microsoft Diagnostic Tool (MSDT) simply by opening a Word document. The Follina zero-day provided a new critical attack vector leveraging Microsoft Office programs as it worked without elevated privileges, avoided detection by Windows Defender, and did not require macro code to be enabled to execute binaries or scripts.

The RCE vulnerability appears when MSDT is called over the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can execute arbitrary code with the calling application's privileges. In the context permitted by the user's permissions, the attacker can then install applications, read, update, or remove data, or create new accounts. Microsoft has patched the Windows MSDT flaw in cumulative updates released in June 2022.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

Threat Actors exploiting Follina

Earlier in June, a Chinese threat actor, TA413 group, was spotted exploiting MSDT zero-day, "Follina," to remotely execute malicious code on Windows systems. When victims browsed or previewed Word documents delivered in ZIP packages, it executed malicious code via the MSDT protocol. The campaign pretended to be the Central Tibetan Administration's "Women Empowerment Desk" and registered the domain tibet-gov.web[.]app. Additionally, DOCX files with Chinese filenames were discovered; this form of malware, which delivers a malicious payload, is recognized as a password-stealing Trojan.

A one-of-a-kind phishing campaign used publicly available Follina exploits to acquire RCE and spread the Rozena backdoor on Windows PCs. It's a backdoor that can launch fileless attacks, use the public Discord CDN attachment service, and inject a remote shell connection back to the attacker's device. The initial vector is a weaponized Office document that, when opened, connects to a Discord CDN URL to receive an HTML file ("index.htm"), which then launches a diagnostic tool using a PowerShell command to download subsequent payloads from the same CDN. The malware's primary purpose is to inject a shellcode that launches a reverse shell to the attacker's hosted website, allowing control of system monitoring and collecting data while also maintaining a backdoor to the compromised system.

Later, APT40 was specified using an actor-controlled domain to deploy the malware, which also exploited malicious RTF files to launch a first-stage downloader

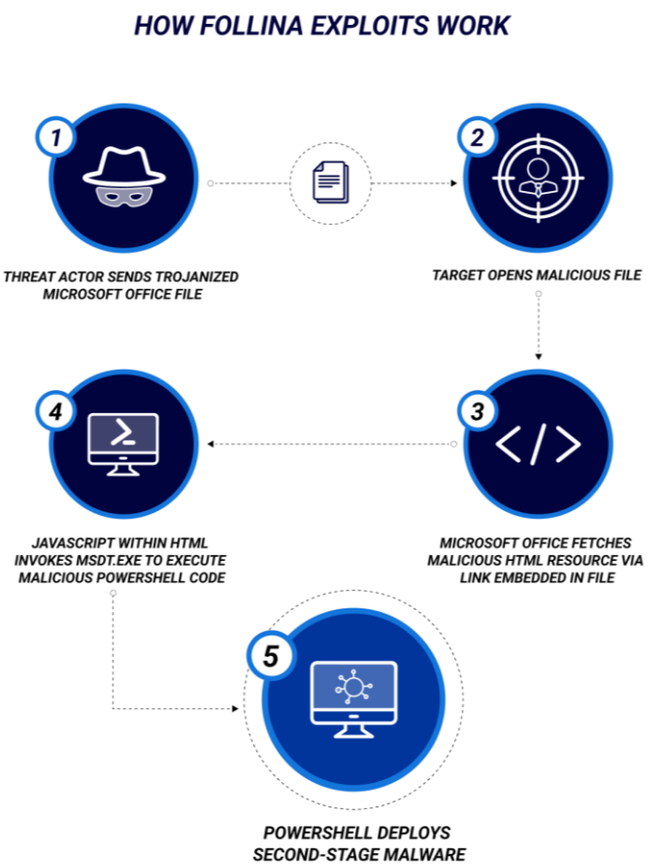

Figure 1: How Follina Exploit Works | Source - Blackberry

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

that functioned as a conduit for receiving encoded versions of the Meterpreter shellcode. The threat actor would typically pose as a representative of the fictitious "Australian Morning News," sending out URLs to the malicious domain and demanding that targets view or share any published research information.

Recently, TA570 used the Follina vulnerability to initiate a Qbot infection chain and gain unauthorized access to the systems. Qbot is a well-known banking Trojan that can conduct reconnaissance, lateral movement, data exfiltration, and payload delivery while acting as an initial access broker. The initial access in this attack was achieved by a malicious Word document laced with Follina exploit code and delivered via phishing email. When the Word document is executed, a remote server retrieves an HTML file carrying a PowerShell payload. The payload is base64-encoded code that downloads Qbot DLLs in the victim's Temp directory. The Qbot DLL is executed by Regsvr32.exe and injected into a trustworthy process (explorer.exe).

By evaluating these campaigns that rely on the MSDT exploit, we can infer that Follina is being used to deliver payloads associated with persistent threat actors, such as Cobalt Strike, Mimikatz, and customized malware. Follina improves attackers' capability to operate in compromised environments while evading detection by leveraging a commonly used module, MSDT. It can use PowerShell to perform lateral movement and data exfiltration within infiltrated environments. These complex assault tactics demonstrates the attackers' concentrated efforts to circumvent detection.

Aside from updating vulnerable systems, security and threat hunting teams should become acquainted with the Follina trojan and take steps to monitor for activities inside their environment that may suggest hostile actors are seeking to employ the Follina vulnerability against them.

Analysis: Affected Products and Versions

- Windows 10 - 1607, 1809, 20H2, 21H1, 21H2 and Windows 11, 7, 8.1, and RT 8.1.
- Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 and 20H2.

CVE ID	Severity	CVSS Score
CVE-2022-30190	High	7.8

Detection

Utilize the below YARA rules to detect Follina infections in the network:

- Rule for process creation
- Domain Trust Discovery
- New Lolbin Process by Office Applications

KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

- Sdiagnhost Calling Suspicious Child Process
- Registry Defender Exclusions
- Esentutl Steals Browser Information
- Network Reconnaissance Activity
- Atera Agent Installation
- FromBase64String Command Line
- Scheduled Task Executing Powershell Encoded Payload from Registry
- CobaltStrike Named Pipe
- SplashTop Network
- SplashTop Process

Recommendations

- Refer to the Microsoft's Security Advisory for CVE-2022-30190 and apply the mentioned patch to the affected versions.
- As a protective measure, prevent unnecessary PowerShell or Batch files execution by implementing policies and standards that permit only signed scripts to execute.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Check the sender's identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Continuously monitor for anomalous activities, including suspicious activity in the temp folder and the download or installation of unauthorized applications. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Perform regular data backup procedures and maintain up-to-date incident response and recovery procedures.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.
- Enable logging mechanisms in critical infrastructure and periodically review them for configuration changes
- Utilize the above mentioned YARA rules to detect Follina attacks in the network.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

- In case the patches are delayed, follow the workaround to disable MSDT URL protocol. It will prevent troubleshooters being launched as links throughout the OS.
  - **To disable the MSDT URL Protocol**
    1. Run Command Prompt as Administrator.
    2. To back up the registry key, execute the command “reg export HKEY_CLASSES_ROOT\ms-msdt filename“
    3. Execute the command “reg delete HKEY_CLASSES_ROOT\ms-msdt /f”.
  - **To undo the workaround**
    1. Run Command Prompt as Administrator.
    2. To back up the registry key, execute the command “reg import filename”.

References

- KPMG - Cyber Threat Notification - New MS Office attack vector exploits Diagnostic Tools for RCE, 31st May 2022, Tracker ID - TN0528
- KPMG Cyber Threat Notification, TA570 QBot Exploits Follina for Domain Compromise, 10th Nov 2022, Tracker ID- TN1108
- KPMG Cyber Threat Notification, ScanBox Framework used for Cyber Espionage by Chinese Threat Actors, 06th Sep 2022, Tracker ID- TN0904
- KPMG Cyber Threat Notification, DoNot Team revamped Jaca Windows malware toolkit, 02nd Sep 2022, Tracker ID- TN0908
- KPMG Cyber Threat Notification, Follina bug exploited to deploy Rozena Backdoor, 13th July 2022, Tracker ID- TN0714
- KPMG Cyber Threat Notification, Follina MSDT zero-day exploited by Chinese APTs, 01st June 2022, Tracker ID- TN0529
- Follina Exploit Leads to Domain Compromise, The DFIR Report, 31st October 2022, External Link (thedfirreport.com).
- MSRC, Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability, Microsoft, 30th May 2022, External Link (msrc[.]microsoft[.]com)
- CISA, Microsoft Releases Workaround Guidance for MSDT "Follina" Vulnerability, National Cyber Awareness System, 31st May 2022, External Link (cisa[.]gov).
- Xavier Mertens (Version: 1), SANS, First Exploitation of Follina Seen in the Wild, 31st May 2022, External Link (isc[.]sans[.]edu).
- Ravie Lakshmanan, Microsoft Releases Workarounds for Office Vulnerability Under Active Exploitation, 31st May 2022, External Link (thehackernews[.]com).

KPMG Cyber Threat Intelligence Platform

Cyber Threat Digest | Threat Analysis of Widely Exploited CVE-2022-30190 - Follina Vulnerability

Tracker ID: TD1201 **Date:** December 07, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

- Sergiu Gatlan, Windows MSDT zero-day now exploited by Chinese APT hackers, Bleeping Computer, 31st May 2022, External Link (www[.]bleepingcomputer[.]com).
- Ravie Lakshmanan, Hackers Exploiting Follina Bug to Deploy Rozena Backdoor, 09th July 2022, Hacker News, External Link (thehackernews.com).
- Blackberry, The Follina Vulnerability: A Guide, External Link (www.blackberry.com).
- Cara Lin, From Follina to Rozena - Leveraging Discord to Distribute a Backdoor, 06th July 2022, Fortinet, External Link (fortinet.com).
- Ravie Lakshmanan, DoNot Team Hackers Updated its Malware Toolkit with Improved Capabilities, The Hacker News, 19th August 2022, External Link (thehackernews.com).
- HIDO COHEN, APT-C-35 GETS A NEW UPGRADE, Morphisec, 11th August 2022, External Link (blog.morphisec.com).
- MICHAEL RAGGI AND SVEVA SCENARELLI, Rising Tide: Chasing the Currents of Espionage in the South China Sea , Cybereason, 30th August 2022, External Link (proofpoint.com).
- Ravie Lakshmanan, Chinese Hackers Used ScanBox Framework in Recent Cyber Espionage Attacks, 31st August 2022, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471