CVE-2022-30190: Microsoft Support Diagnostic Tool (MSDT) RCE Vulnerability “Follina”

fortinet.com/blog/threat-research/analysis-of-follina-zero-day

June 1, 2022

At the end of last week, @nao_sec, an independent cyber security research team, tweeted about a malicious Microsoft Word document submitted from Belarus that leverages remote templates to execute a PowerShell payload using the "ms-msdt" MSProtocol URI scheme. Additional developments over the weekend identified the issue as a new unpatched vulnerability in Windows. A successful attack results in a remote, unauthenticated attacker taking control of an affected system. A publicly available Proof-of-Concept soon followed.

This issue is referred to as “Follina’ and has a CVE assignment of CVE-2022-30190.

The name of the vulnerability is credited to security researcher Kevin Beaumont. "Follina" was derived from his analysis of the 0-day that contained code referencing "0438", which is the area code of Follina, Italy. Most of the time, it’s a bad sign when a vulnerability is

crowned with a unique name (having a mind-shaking logo is usually the last dagger – such as Heartbleed, Shellshock, and EternalBlue, but thankfully, this issue is not in the same league as those.

As FortiGuard Labs is on high watch for updates and developments for CVE-2022-30190, this blog intends to raise awareness of this critical vulnerability and to urge administrators and various organizations to take quick corrective action until Microsoft releases a patch.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Full Control of Affected Machine
Severity level: Critical

Impact Assessment

The first question you probably would ask is how bad this vulnerability is. CVE-2022-30190 is rated as CVSS 7.8 (Critical), and there are a number of reasons for it.

This vulnerability is in the Microsoft Support Diagnostic Tool (MSDT), a tool from Microsoft that collects and sends system information back to Microsoft Support for problem diagnostics, such as issues with device drivers, hardware, etc. This tool is in all versions of Windows, including Windows Server OS. Because of the lack of an available patch from Microsoft (as of June 1st, 2022), machines that are not protected by endpoint software or a mitigation strategy are vulnerable to Follina.

As proof-of-concept code is publicly available, this code can be freely used by security researchers, administrators, and threat actors alike. As such, attacks that leverage CVE-2022-30190 are expected to increase over the next few days and weeks.

Protected View, a feature in Microsoft Office that opens Office documents in read-only mode with macros and other content disabled, can prevent this attack. However, reports from researchers have revealed that if a document is converted to Rich Text Format (RTF) format, simply previewing the document in Windows Explorer can trigger the exploit, bypassing Protected View. At the time of writing, Microsoft's latest advisory has not confirmed this nor whether this is another exploitation vector.

On a side note, despite using "remote" in the vulnerability name, the attack happens locally, and user interaction is required for the attack to work. Microsoft's advisory calls out this point: "The word Remote in the title refers to the location of the attacker. This type of exploit is sometimes referred to as Arbitrary Code Execution (ACE). The attack itself is carried out locally."

Additionally, the vulnerability has already experienced in-the-wild attacks. As shown in the timeline at the end of this blog (see Timeline), a series of initial attacks were reportedly observed in March 2022, targeting the Philippines, Nepal, and India. Additional files were

submitted to VirusTotal from Russia and Belarus. Those attacks were most likely targeted attacks as the domains involved reveal little activity in our telemetry.

Due to the severity of the vulnerability, the United States Cybersecurity & Infrastructure Security Agency (CISA) issued an advisory on May 31st, urging users and administrators to apply necessary workarounds as soon as possible.

Exploit

The vulnerability that exists within msdt.exe is the Microsoft Support Diagnostic Tool. Normally, this tool is used to diagnose faults with the operating system and then report and provide system details back to Microsoft Support.

Figure 1. The Microsoft Support Diagnostic Tool as is meant to be seen.

The vulnerability allows a malicious actor to effectively execute arbitrary code with the same privileges as the application calling it. As has been the case with the original reporting of this from @nao_sec and subsequent experimentation in the wider security community, the calling application is quite often a tool in Microsoft Office (Word, Excel, Outlook, etc.).

The original document and subsequent HTML file can be found here and here.

Figure 2. Original OLE object showing the download location of the subsequent HTML file.

As shown in Figure 2, the document found by @nao_sec used an embedded OLE Object inside a Word document that was modified to call an external website to download an HTML document. This document then invoked msdt.exe, followed by several PowerShell commands.

Figure 3. HTML file invoking MSDT.

Figure 3 shows the original HTML payload, which required several lines with the letter 'A' (61) to be commented out of the script in order to execute. MSDT was then invoked using character and Base64 encoding to obfuscate the actual command.

Figure 4. Decoded command.

Many further examples have been uploaded to VirusTotal that invoke Calc and other benign Windows tools as a method to test the vulnerability without causing damage.

Active Exploitation

The TA413 APT group, a hacking outfit linked to Chinese state interests, has adopted this vulnerability in attacks against the international Tibetan community. As observed on May 30 by security researchers, threat actors are now using CVE-2022-30190 exploits to execute

malicious code via the MSDT protocol when targets open or preview Word documents delivered in ZIP archives. Campaigns have impersonated the 'Women Empowerments Desk' of the Central Tibetan Administration and use the domain tibet-gov.web[.]app.

The security researchers also spotted DOCX documents with Chinese filenames being used to install malicious payloads detected as password-stealing Trojans via "hxxp://coolrat[.]xyz".

At the time of writing, researchers have discovered limited exploitation of the vulnerability in the wild. One instance of active exploitation of 'Follina' was conducted by Chinese APT actor 'TA413'.

Attack Vector

At the time of this writing, all known attacks used Microsoft Word document files that were most likely delivered via email. Theoretically, any applications that allow an OLE object to be embedded would be a viable execution mechanism.

In the Wild Attack

One of the real-world attacks that leverage CVE-2022-30190 is a Microsoft Word file submitted to VirusTotal from Saudi Arabia on June 1st (SHA2: 248296cf75065c7db51a793816d388ad589127c40fddef276e622a160727ca29), which MalwareHunterTeam posted in a tweet:

Figure 5. Malicious Word file that was used in an attack leveraging CVE-2022-30190.

The doc file retrieves an HTML file from 212[.]138[.]130[.]8/analysis.html, which abuses MSDT to fetch the next stage payload “svchost.exe” from a remote location and then execute it.

Figure 6. Contents of retrieved analysis.html

Payload Analysis

The Saudi Arabian DOCX document eventually leads to the download and execution of an executable. This executable (SHA256: 4DDA59B51D51F18C9071EB07A730AC4548E36E0D14DBF00E886FC155E705EEEF) is a variant of Turian, which was analyzed by ESET (https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) almost a year ago. This current variant uses the same one-byte XOR key (0xA9) as the previously analyzed Turian sample.

Figure 7. XOR key 0xA9 used for decryption

This sample also has the functionality to try and determine what role the infected computer plays in the domain.

Figure 8. Functionality to determine domain role

Similar to the old Turian sample, this variant uses the same headers to connect to the C2 server.

Figure 9. Connection headers

This sample creates “tmp.bat”, which is used to set RUN keys in the registry for persistence purposes.

Figure 10. Content of the”tmp.bat” file

Note the mixed usage of upper and lowercase letters, which is the same as the old Turian sample.

This latest variant uses www[.]osendata[.] com as its C2 server.

Another Turian sample similar to this latest variant has a SHA256 hash of 34DC42F3F486EC282C5E3A16D81A377C2F642D87994AE103742DF5ED5804D0F7 and a C2 server of www[.]tripinindian[.]com.

Mitigation

Microsoft has provided the following mitigation steps in a blog posted on May 30th, 2022.

CISA also urged admins and users to disable the MSDT protocol on their Windows devices after Microsoft reported active exploitation of this vulnerability in the wild.

Disabling the MSDT URL Protocol:

Disabling the MSDT URL protocol prevents troubleshooters from being launched as links, including links throughout the operating system. Troubleshooters can still be accessed using the Get Help application and in System Settings as other or additional troubleshooters. Follow these steps to disable:

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”.

Figure 11. ms-msdt in Registry Editor

How to undo the workaround

1. Run Command Prompt as Administrator.
2. To restore the registry key, execute the command “reg import filename”

Timeline

Timeline of CVE-2022-30190 based on information gathered by FortiGuard Labs: *(updated June 2)*

Year	Month/Date	Event
2022	April 12th	crazyman_army with an APT hunting team “Shadow Chaser Group,” reported the vulnerability to Microsoft. The report was based on a Word document file that appears to have been used in a real attack targeting Russia.
April 21st	Microsoft determined that it was not a security-related issue.	
May 27th	nao_sec, an independent cyber security research team, tweeted about a malicious Microsoft Word document file submitted from Belarus that leverages remote templates to execute the PowerShell payload using the "ms-msdt" MSProtocol URI scheme.	
May 30th	• Kevin Beaumont, a security researcher known as GossiTheDog, posted a blog citing that this is an unpatched vulnerability. • CVE-2022-30190 was assigned to the vulnerability.	

Conclusion

CVE-2022-30190 has the potential to have significant impact due to its ease of exploitation and ability to bypass Protected View, along with the availability of new PoC code and the lack of a security fix. Administrators and users should monitor updates from Microsoft and apply the patch as soon as it becomes available. Until then, mitigation should be applied as soon as possible.

Fortinet Protection

The FortiGuard Antivirus service detects and blocks files associated with CVE-2022-30190 with the following signatures:

HTML/CVE_2022_30190.A!tr

MSWord/Agent.2E52!tr.dldr

MSWord/CVE20170199.A!exploit

Riskware/RemoteShell.

Regarding IPS coverage, the following signature will detect the retrieval of remote HTML files that contain the MSDT command:

MS.Office.MSHTML.Remote.Code.Execution.

The FortiGuard Content Disarm and Reconstruction (CDR) service can detect the attack in real-time and prevent it by disarming the "oleobject" data from Microsoft Office files.

All relevant URLs have been rated as "Malicious Websites" by the FortiGuard Web Filtering service.

For a comprehensive list of Fortinet technologies that prevent exploitation of CVE-2022-30190, please refer to our Outbreak Alert Service page, “MSDT Follina.”

As these attacks require user interaction, it is also suggested that organizations regularly schedule user awareness and training simulations on how to spot a social engineering attack. Fortinet has multiple solutions designed to train users on how to understand and detect phishing threats:

FortiEDR detects post-exploitation behavior associated with the CVE-2022-30190 vulnerability. A KB article detailing how FortiEDR can mitigate this issue can be found here.

We suggest that organizations have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats to train end-users on how to identify and protect themselves from phishing attacks.

In addition, the FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and train and reinforce proper practices when users encounter targeted phishing attacks.

IOCs

Files:

710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa

fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45

3db60df73a92b8b15d7885bdcc1cbcf9c740ce29c654375a5c1ce8c2b31488a1

4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784

d118f2c99400e773b8cfd3e08a5bcf6ecaa6a644cb58ef8fd5b8aa6c29af4cf1

764a57c926711e448e68917e7db5caba988d3cdbc656b00cd3a6e88922c63837

8e986c906d0c6213f80d0224833913fa14bc4c15c047766a62f6329bfc0639bd

e8f0a2f79a91587f1d961d6668792e74985624d652c7b47cc87367cb1b451adf

4369f3c729d9bacffab6ec9a8f0e582b4e12b32ed020b5fe0f4c8c0c620931dc

1f245b9d3247d686937f26f7c0ae36d3c853bda97abd8b95dc0dfd4568ee470b

bf10a54348c2d448afa5d0ba5add70aaccd99506dfcf9d6cf185c0b77c14ace5

c0c5bf6fe1d3b23fc89e0f8b352bd687789b5083ca6d8ec9acce9a9e2942be1f

248296cf75065c7db51a793816d388ad589127c40fddef276e622a160727ca29

d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7

4f11f567634b81171a871c804b35c672646a0839485eca0785db71647a1807df

URL(s):

sputnikradio[.]net
xmlformats[.]com
exchange[.]oufca[.]com[.]au
141[.]98[.]215[.]99
tibet-gov[.]web[.]app

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.