Staying Ahead of CVE-2022-30190 (Follina)

Aleksei Sviridov
Mar 31, 2022

Executive Summary

- Follina RCE bug in Microsoft Windows affects all versions of Windows from Windows Vista onwards. The bug is a remote code execution vulnerability in the msdt.exe component of Microsoft Windows Support Diagnostic Tool (MSDT) and is tracked as CVE-2022-30190.
- Follina allows remote code execution via Microsoft Office documents, which can be delivered via phishing emails or through other means, such as malicious ads.
- Multiple threat actors have been observed exploiting CVE-2022-30190 in the wild, including Chinese APT Gamaredon and cross-platform malware families such as Cobalt Strike and Metasploit.
- SentinelOne Singularity platform detects and blocks the vulnerability. Microsoft recommends users apply the security fix for CVE-2022-30190.

Background

Discovered by researcher Kevin McPeck and first tweeted about by Security Researcher Nao Sec, the bug affects Windows and other products which ship with Microsoft Office.

The vulnerability exploits Microsoft Office's ability to download remote templates for the purpose of loading Microsoft Support Diagnostic Tool (msdt.exe), a CLI utility that ships as part of Windows. The bug allows an attacker to execute code by crafting a special URL.

Discovered Threat Actors

Microsoft has observed multiple threat actors exploiting Follina in the wild, including Chinese APT Gamaredon and other threat actors that have been observed in late March 2022. The list includes Chinese and Russian threat actors of interest.

- Microsoft Security Response Center (MSRC) blog post on Gamaredon's use of Follina exploitation (Twitter thread here)
- Follina exploitation in the wild - on Twitter (thread by @malwarebytes) and Malware Bytes blog post (Gamaredon and Cobalt Strike)
- Gamaredon has been active since at least 2013 and has been attributed to the Russian Federal Security Service (FSB) by the Ukrainian Cyber Alliance.

Mitigation Guidance

Microsoft has released security updates for affected versions of Windows. Microsoft recommends applying the security fix for CVE-2022-30190.

- Follina Workaround - Twitter thread by @cyb3rward0g
- Follina Workaround - Twitter thread by @SecurityJoes

Microsoft has also published a workaround for Follina. Follow the instructions in the following Microsoft Blog.

- Follina Workaround - MSRC blog post

SentinelOne vs CVE-2022-30190 (Follina)

SentinelOne Singularity platform detects and blocks Follina. Follow the steps below to see how it works.

Threat Name: NOT MITIGATED | Classification: RECEIVED | Action Taken: Protected (Quarantined)

Threat Details

NETWORK HISTORY

First seen: May 31, 2022 10:02:50
Last seen: May 31, 2022 10:02:50

0 Times in Cloudwalker
0 Accounts | 0 Sites | 1 Endpoint

THREAT FILE HASH: d3d9446a7a9a

Type	Microsoft Windows Executable Executable (Classifie...
Connection Direction	In, TCP, Listen(1.1.1.1:0)remote(1.1.1.1:0)[1.1.1.1:0]
Process Name	msdt.exe
Process Path	C:\Windows\System32\msdt.exe
Signer Identity	-
Signature Verification	Signed
Originating Process	explorer.exe
SHA1	0d1a4f4f8b3d0b1f2f1a2f8dda2f3d39f3f47b3d0d28b

Watch the video to see how SentinelOne stops the Follina exploit in action. Follow the steps below.

Additional Resources

- Microsoft Security Response Center Blog - Follina Vulnerability
- Malwarebytes Follina Exploitation Blog
- Follina Exploitation Detection Blog - Kevin McPeck
- Twitter thread by @malwarebytes on Follina exploitation in the wild

SOLVE CYBER THREATS in minutes, not days, with SentinelOne. Request a Demo Today!

Read more about Cyber Security:

- Cyber Security Terms - Vulnerability, Threat, Exploit, Malware and Other Cyber Terms
- Ransomware Protection - Ransomware Attack Types and Ransomware Protection Techniques
- Malware Protection - Malware Types and Malware Protection Techniques
- Cybersecurity Glossary - Cybersecurity Terms and Definitions
- Cyber Attack Types - Cyber Attack Types and Cyber Attack Prevention

Cookie Settings