Hive Pro

Threat Level

Red

THREAT ADVISORY

# ATTACK REPORT

# Follina: A zero-day vulnerability in Microsoft Office

| Date of Publication | Last Updated Date | Admiralty code | TA Number |
| --- | --- | --- | --- |
| May 31, 2022 | June 15, 2022 | A1 | TA2022109 |

# Summary

Microsoft has issued a patch after almost 15 days for a zero-day vulnerability identified as CVE-2022-30190 after various proof-of-concept (POCs) indicating that it is actively exploited became public. Security researchers have also named this security flaw as Follina. A Chinese actor group, TA413 is been observed targeting organizations in Tibet with a malicious document with Follina.

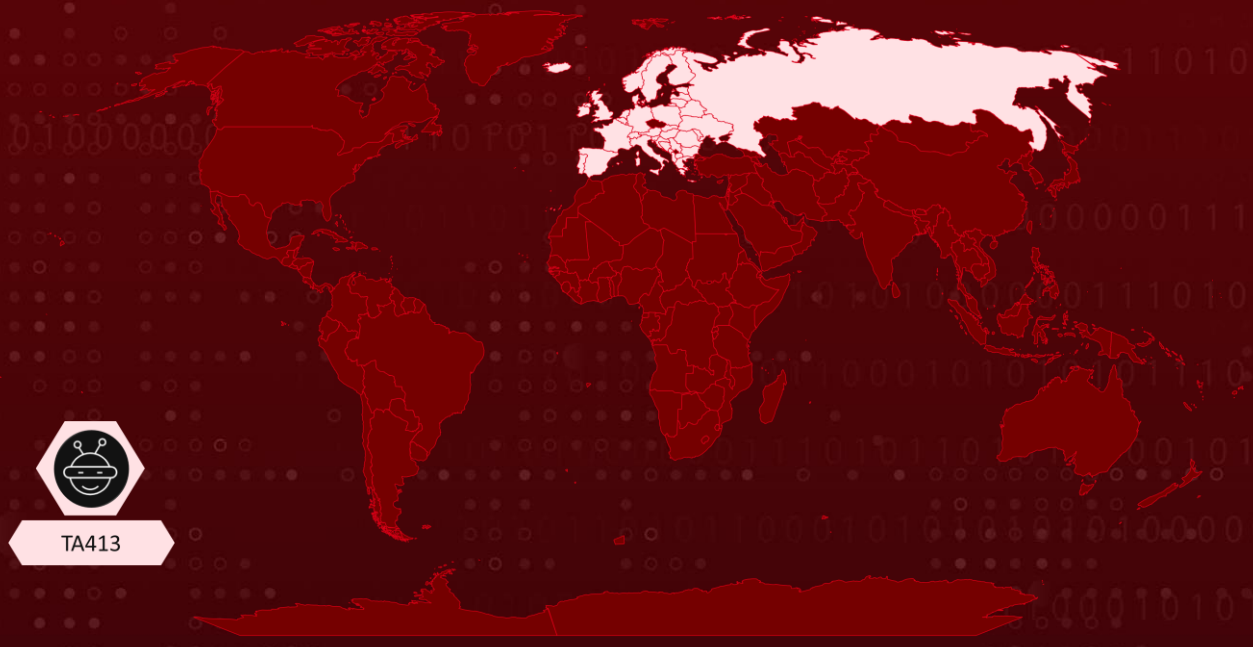
## CVE

| CVE | NAME | PATCH |
|---|---|---|
| CVE-2022-30190 | Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability | ✓ |

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution | **TA0005** Defense Evasion |
| **T1588** Obtain Capabilities | **T1588.006** Obtain Capabilities: Vulnerabilities | **T1588.005** Obtain Capabilities: Exploits | **T1566** Phishing |
| **T1566.001** Phishing: Spearphishing Attachment | **T1564** Hide Artifacts | **T1564.003** Hide Artifacts: Hidden Window | **T1059** Command and Scripting Interpreter |
| **T1059.001** Command and Scripting Interpreter: PowerShell | **T1204** User Execution | **T1204.002** User Execution: Malicious File | |

# Actor Map


TA413
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Wikipedia

# Technical Details

**#1**

Follina (CVE-2022-30190) is a remote code execution(RCE) vulnerability that occurs when Microsoft Support Diagnostic Tool (MSDT) is called using the URL protocol in Office Applications such as Word, Excel, PowerPoint.

**#2**

The attack begins with sending documents over email or through a website link that hosts the document. As soon as the victim downloads the document this zero-click exploits gets executed.

**#3**

An official patch is available now. However, the following mitigations could be followed to if organizations cannot update right away

- Enable Protected View for all Microsoft documents
- Disable the preview pane in Windows Explorer
- Remove the ms- msdt protocol handler

## Vulnerability Details

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2022-30190 | Windows Server: 2008 – 2022 & Windows: 7 - 11 21H2 | cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* | CWE-78 |

## Actor Detail

| NAME | ORIGIN | MOTIVE | TARGET LOCATIONS | TARGET INDUSTRIES |
|---|---|---|---|---|
| TA413 | China | Information theft and espionage | Tibet and Europe | Diplomats, Government, non-profit organizations, and non-governmental organization |

# Indicator of Compromise (IOC)

| TYPE | VALUE |
|---|---|
| MD5 | 52945af1def85b171870b31fa4782e52, f531a7c270d43656e34d578c8e71bc39, 6bcee92ab337c9130f27143cc7be5a55, 529c8f3d6d02ba996357aba535f688fc |
| SHA1 | 06727ffda60359236a8029e0b3e8a0fd11c23313, 934561173aba69ff4f7b118181f6c8f467b0695d, 447139a8cfc9660215bef2230e25885f553ddba8, f5978deec22543a301e7ff4e01db950d8f474a4c |
| SHA256 | 4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784, 710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa, fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45, d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7 |

# Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

# References

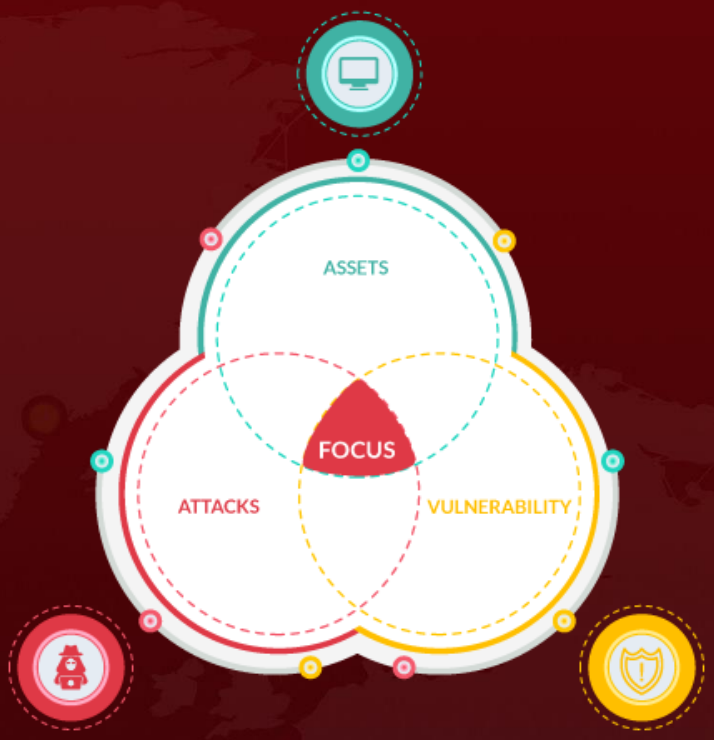
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e

https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-_msdt-bug

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.




At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**May 31, 2022. 7:00 AM**



More at www.hivepro.com