



FLASH

FOLLINA VULNERABILITY

ZEROFOX INTELLIGENCE

F-2022-06-01a

Classification: White

Criticality: High

Intelligence Requirements: Vulnerability, Deep Dark Web & Criminal Underground

June 1, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EDT) on June 2, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Follina Vulnerability

Key Findings

- The identified vulnerability, dubbed Follina, affects all versions of Windows still receiving security updates and has been designated as CVE-2022-30190.
- Chinese advanced persistent threat (APT) group TA413 has already been observed exploiting the Follina vulnerability.
- Disabling macros in Word does not prevent the exploit from being triggered; the payload can be initiated by opening a Word Document.
- CVE-2022-30190 can be triggered by viewing a weaponized Word document saved in Rich Text Document form in the Explorer preview pane.
- Workarounds are available.

Analyst Commentary

On May 27, 2022, security researcher “nao_sec” shared a malicious Word document that had been discovered taking advantage of Windows’ Microsoft Support Diagnostic Tool (MSDT). The document abused Microsoft Word’s ability to load remote document templates to retrieve a HTML file from a web server. The retrieved HTML document contained embedded JavaScript to trigger ms-msdt protocol via a `window.location.href` reference to execute a PowerShell script.¹ PowerShell is a cross-platform command line interpreter and scripting language created by Microsoft that is installed by default in Windows. This vulnerability, dubbed “Follina,” has been used in the wild. For example, a known Chinese APT, TA413, has been observed exploiting Follina while impersonating the “Women Empowerments Desk” of the Central Tibetan Administration.²

Microsoft has been aware of this vulnerability since April 2022, when another security researcher using the handle “crazyman” submitted a report about the exploit. Follina has been designated as CVE-2022-30190.

¹ <https://github.com/chvancooten/follina.py/blob/main/follina.py>

²

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



Recommendations

Microsoft shared instructions for an official workaround through the Microsoft Security Response Center (MSRC) website on May 30, 2022.³ To disable the MSDT protocol handler, Microsoft suggests the following steps:

1. Open Command Prompt as an administrator.
2. Run “reg export HKEY_CLASSES_ROOT\ms-msdt filename”, with “filename” being the name of the file that will be created as a backup.
3. Run “reg delete HKEY_CLASSES_ROOT\ms-msdt /f” to delete the registry key.

To restore this functionality, administrators can once again open Command Prompt as an administrator and then run “reg import filename” where “filename” is the name of the backup file created earlier.

In addition to Microsoft’s instructions, the following recommendations should also be considered.

- Ensure antivirus and intrusion detection software is up to date with all patches and rule sets.
- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Avoid opening unsolicited attachments and never click suspicious links.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Review network logs for potential signs of compromise and data egress.

3

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



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:

WHITE information without restriction, subject to copyright controls.