CERT-EU

Security Advisory 2022-039

Follina Vulnerability in Microsoft Office Products

June 15, 2022 — v1.3

TLP:WHITE

History:

- *30/05/2022 — v1.0 – Initial publication*
- *31/05/2022 — v1.1 – Updated with new information available*
- *02/06/2022 — v1.2 – Updated with new information available about* `search-ms`
- *15/06/2022 — v1.3 – Updated with new information about Microsoft patch*

Summary

On the 29th of May 2022, the Nao_Sec team [1], an independent Cyber Security Research Team, discovered a malicious Office document shared on Virustotal [2]. This document is using an unusual, but known scheme [3] to infect its victims. The scheme was not detected as malicious by some EDR, like Microsoft Defender for Endpoint. This vulnerability could lead to code execution without the need of user interaction, as it does not involve macros, except if the `Protected View` mode is enabled and the `Preview mode` is disabled in Windows Explorer [4].

On the 30th of May 2022, Microsoft started to track this vulnerability identified `CVE-2022-30190` (aka Follina) with a severity score of 7.8 out of 10.

On the 14th of June 2022, Microsoft has released security updates as part of June Patch Tuesday. One of the fixes applies to this actively exploited vulnerability. This update does not prevent Microsoft Office tools from loading Windows protocol URI handlers without user interaction, but will instead block PowerShell injection and disable this attack vector [16].

Technical Details

The vulnerability is being exploited by using the `MSProtocol URI` scheme to load some code. Attackers could embed malicious links inside Microsoft Office documents, templates or emails beginning with `ms-msdt:` that will be loaded and executed afterward without user interaction - except if the `Protected View` mode is enabled and/or the `Preview mode` is disabled in Windows Explorer [5]. Nevertheless, converting the document to the RTF format could also bypass the `Protected View` feature.

Security researchers have shown that it is possible to exploit this vulnerability with another `MSProtocol URI` scheme: `search-ms:`. Using this scheme, attackers would be able to automatically mount remote shares on a computer in order to trick the user into executing malware [14].

Affected Products

The flow is affecting all Windows version still receiving Security Updates [11].

Recommendations

CERT-EU strongly recommends installing the last updates provided with June 2022 cumulative Windows Updates.

Enabling `Protected View` and disabling `Preview Mode` is still recommended.

Monitoring

CERT-EU highly recommends monitoring for suspicious behaviours of Microsoft Office products: the process `msdt.exe` should not be spawned by Office products like `words.exe`, `outlook.exe` and also `excel.exe`.

Some researchers have released monitoring rules for various products:

- Sigma [6]
- Sentinel [7]
- Defender [8]

Workarounds

Note: The workarounds described below are to be implemented if updating is not an option.

As a temporary workaround, Didier Stevens proposed to remove the `ms-msdt` handler in the registry hives. While this could prevent legitimate applications to work, it seems that there are not many applications using it [9]. Microsoft also provided this word around [13].

The same way as for the MSDT mitigation, it is possible to delete the `search-ms` protocol handler from the Windows Registry [15].

It is also possible to use the Attack Surface Reduction features to prevent Office applications from spawning child processes [10]. However, some legitimate line-of-business applications might also generate child processes for benign purposes and will be blocked if enabled.

References

[1] https://nao-sec.org/about

[2] https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection

[3] https://blog.syss.com/posts/abusing-ms-office-protos/

[4] https://youtu.be/GybD70_rZDs

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

[6] https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_msdt.yml

[7] https://github.com/le0li9ht/Microsoft-Sentinel-Queries/blob/main/Detect-Follina-Exploitation.kql

[8] https://github.com/GossiTheDog/ThreatHunting/blob/master/AdvancedHuntingQueries/Follina-Office.ahq

[9] https://twitter.com/sans_isc/status/1531075423270051841?s=20&t=_NYOie6ydEbP4JT5zHVJ7A

[10] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-all-office-applications-from-creating-child-processes

[11] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

[12] https://twitter.com/wdormann/status/1531427345143320576

[13] https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-mitigation-for-office-zero-day-exploited-in-attacks/

[14] https://twitter.com/hackerfantastic/status/1531789430922567681

[15] https://www.bleepingcomputer.com/news/security/new-windows-search-zero-day-added-to-microsoft-protocol-nightmare/

[16] https://www.bleepingcomputer.com/news/security/microsoft-patches-actively-exploited-follina-windows-zero-day/