Understanding WinRAR Code Execution Vulnerability: CVE-2023-38831 (Part-1)

On 23rd August 2023, the Group-IB Threat Intelligence Unit released a blog where they identified a zero-day vulnerability in WinRAR (CVE-2023-38831) being exploited by Threat Actors in the wild since April 2023, you can go through the blog for better understanding.

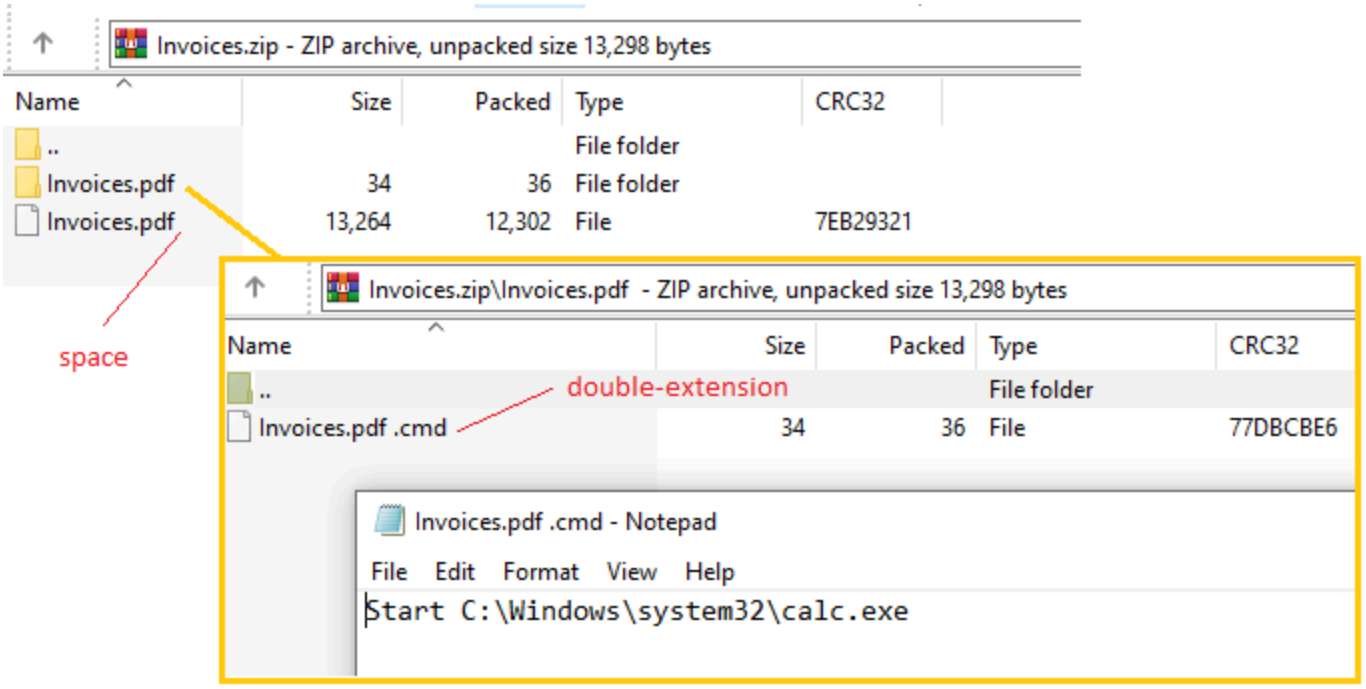
After reversing the vulnerable version of WinRAR & the weaponized ZIP archive for a few hours I was able to reproduce the WinRAR Code Execution Vulnerability (CVE-2023-38831) as shown below

PoC: https://twitter.com/knight0x07/status/1695146888612417913

As seen in the PoC, when the victim opens “Invoices.pdf” from a vulnerable version of WinRAR the calculator is been spawned by exploiting the WinRAR code execution vulnerability

The Weaponized ZIP Archive requires only two things to exploit the vulnerability and execute the malicious code as shown below:

- A space after Invoices.pdf file & the folder -> **"Invoices.pdf "** (File/Folder name could be anything but should be identical for both)
- The **"Invoices.pdf "** folder consists of a file with the malicious code to be executed, the file name in this case should be identical as the previous file/folder but with double extension and space at the end. (Not Necessary) -> **"Invoices.pdf .cmd "**
- Now when the **"Invoices.pdf "** is opened from a vulnerable WinRAR, the "Invoices.pdf .cmd " is executed by exploiting the vulnerability eventually spawning calc.exe

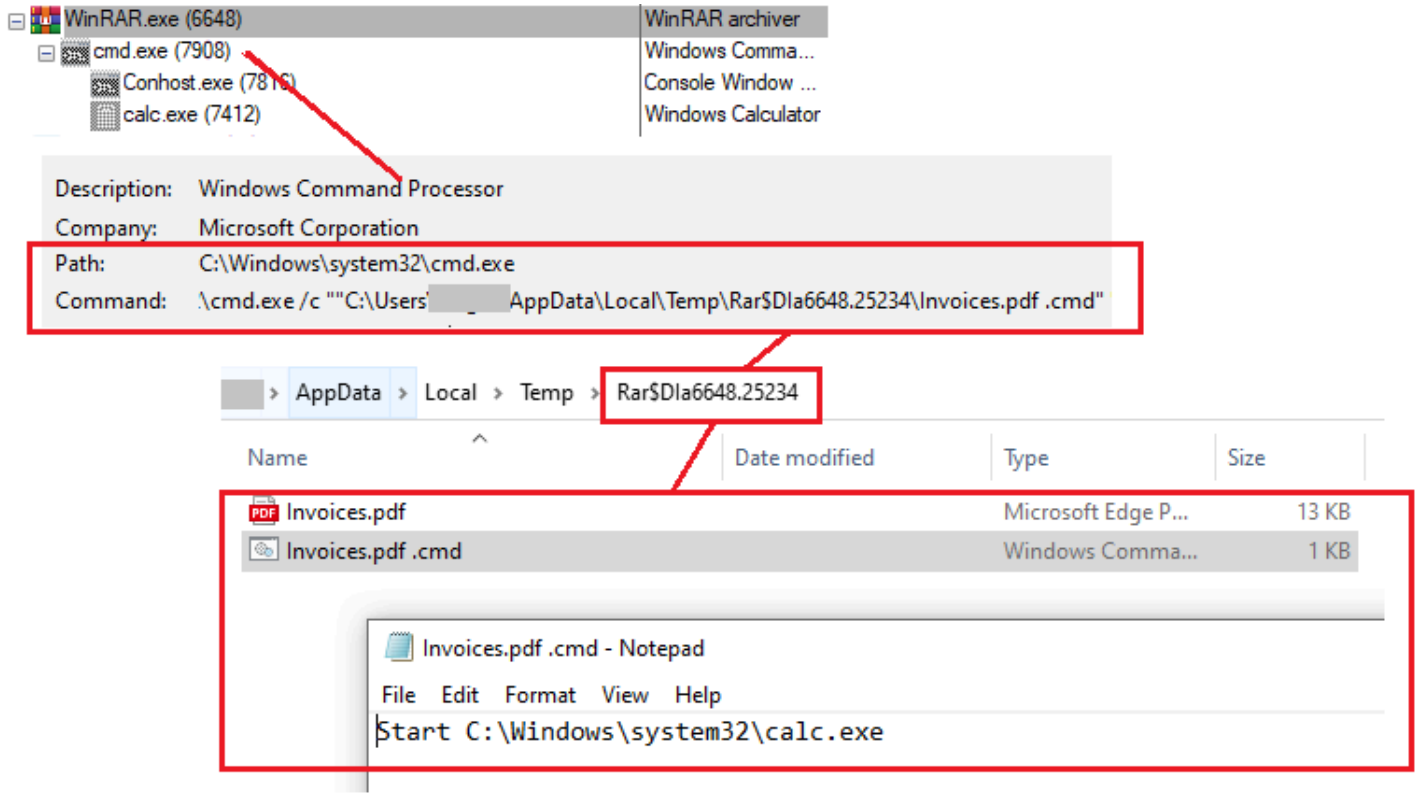


The following anomalies can be leveraged to detect the weaponized ZIP Archives

Note: The reason for such setup of the files in the weaponized ZIP Archive will be explained in the **Part-2 of this post** where we **deep dive and reverse engineer the vulnerability & understand the working =) Stay tuned!**

Now once the **"Invoice.pdf "** is opened, the **"Invoices.pdf .cmd"** is executed from the RAR Temp folder by exploiting the Code Execution Vulnerability and then spawning calc.exe

Process Tree:



WinRAR.exe -> "cmd.exe /c C:\Users<user>\AppData\Local\Temp\Rar$DIa6648.25234\Invoices.pdf .cmd"

Here the RAR Temp folder "Rar$DIa6648.25234" consists of the extracted "Invoices.pdf" and the "Invoices.pdf .cmd" (malicious script - spawning calc.exe)

The following behaviour of WinRAR spawning cmd.exe to execute a file from the RAR Temp folder with double extension can be leveraged for detection purposes + dropping of a file (Operation: CreateFile) with double extension in the RAR Temp Folder can be detected

---

Thanks & Stay tuned for Part-2 of this post where we reverse engineer & understand the WinRAR Code Execution Vulnerability (CVE-2023-38831) in detail.

~ knight0x07

Contact:

- Twitter: https://twitter.com/knight0x07
- LinkedIn: https://www.linkedin.com/in/niraj-s
- Website: https://knight0x07.github.io