

# Lab13

Navya K  
18bcn7048  
L39+L40

TOPIC : Automated Vulnerability Analysis and Patch

## Management

- Downloading the required files from github
- After that click setup.py to set up wes-ng
- Using cmd we will find the exploit and fix it
- First you have to create a systeminfo text file.

```

C:\Users\user\Desktop\wesng-master\wesng-master>systeminfo >systeminfo_sc_lab.txt
C:\Users\user\Desktop\wesng-master\wesng-master>dir
Volume in drive C has no label.
Volume Serial Number is A0D4-F368

Directory of C:\Users\user\Desktop\wesng-master\wesng-master

11-06-2021  20:30    <DIR>          .
11-06-2021  20:30    <DIR>          ..
08-06-2021  00:36             1,760 .gitignore
08-06-2021  00:36             3,166 CHANGELOG.md
08-06-2021  00:36             3,760 CMDLINE.md
08-06-2021  00:36    <DIR>        collector
11-06-2021  20:28       1,461,713 definitions.zip
08-06-2021  00:36       688,951 demo.gif
08-06-2021  00:36             1,458 LICENSE.txt
08-06-2021  00:36             5,629 muc_lookup.py
08-06-2021  00:36             4,864 README.md
08-06-2021  00:36             1,727 setup.py
11-06-2021  20:30             4,166 systeminfo_sc_lab.txt
08-06-2021  00:36    <DIR>        validation
08-06-2021  00:36       31,016 wes.py

```

- Now update wes.py file
- Now run the wes.py file with systeminfo.txt file to find vulnerabilities
- Now find one exploit to patch

```

C:\Users\user\Desktop\wesng-master\wesng-master>python wes.py --update
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitcadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210607

```

```

C:\Users\user\Desktop\wesng-master\wesng-master>python wes.py -e systeminfo_sc_lab.txt
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 ins
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 10 Version 2004 for x64-based Systems
  - Generation: 10
  - Build: 19041
  - Version: 2004
  - Architecture: x64-based
  - Installed hotfixes (12): KB4601554, KB5003254, KB4561600, KB4566785, KB4577586, KB4580325, KB458
B4593175, KB4598481, KB5003637, KB5003503
[+] Loading definitions
  - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Applying display filters
[+] Found vulnerabilities

Date: 20210511
CVE: CVE-2021-26419
KB: KB5003173
Title: Scripting Engine Memory Corruption Vulnerability
Affected product: Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.
Date: 20210511

```

```

Date: 20210511
CVE: CVE-2021-26419
KB: KB5003173
Title: Scripting Engine Memory Corruption Vulnerability
Affected product: Internet Explorer 11 on Windows 10 Version 2004 for x64-based
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.

[+] Missing patches: 1
  - KB5003173: patches 2 vulnerabilities
[+] KB with the most recent release date
  - ID: KB5003173
  - Release date: 20210511

[+] Done. Displaying 2 of the 54 vulnerabilities found.

```

Now fix that exploit

```
C:\Users\user\Desktop\wesng-master\wesng-master>python wes.py -e systeminfo_sc_lab.txt -p KB5003173
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 ins
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 10 Version 2004 for x64-based Systems
  - Generation: 10
  - Build: 19041
  - Version: 2004
  - Architecture: x64-based
  - Installed hotfixes (12): KB4601554, KB5003254, KB4561600, KB4566785, KB4577586, KB4580325, KB458
84593175, KB4598481, KB5003637, KB5003503
  - Manually specified hotfixes (1): KB5003173
[+] Loading definitions
  - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found
```