

Secure Coding Lab – 13

Dasari Mohan Amrithesh

18BCN7038

Windows Exploit Suggester - Next Generation (WES-NG):

ES-NG is a tool based on the output of Windows' systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between Windows XP and Windows 10, including their Windows Server counterparts, is supported.

>>wes.py

```
Select Command Prompt
F:\test\wesng>wes.py
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip2 install chardet
usage: wes.py [-u] [--update-wes] [--version] [--definitions [DEFINITIONS]]
              [-p INSTALLEDPATCH [INSTALLEDPATCH ...]] [-d] [-e]
              [--hide HIDDENVULN [HIDDENVULN ...]] [-i IMPACTS [IMPACTS ...]]
              [--s SEVERITIES [SEVERITIES ...]] [-o [OUTPUTFILE]]
              [-muc -lookup] [-h]
              systeminfo [qfile]

Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )

positional arguments:
  systeminfo            Specify systeminfo.txt file
  qfile                 Specify the file containing the output of the 'wmic
                        qfe' command

optional arguments:
  -u, --update           Download latest list of CVEs
  --update-wes           Download latest version of wes.py
  --version              Show version information
  --definitions [DEFINITIONS]
                        Definitions zip file (default: definitions.zip)
  -p INSTALLEDPATCH [INSTALLEDPATCH ...], --patches INSTALLEDPATCH [INSTALLEDPATCH ...]
                        Manually specify installed patches in addition to the
                        ones listed in the systeminfo.txt file
  -d, --usekbdate        Filter out vulnerabilities of KBs published before the
                        publishing date of the most recent KB installed
  -e, --exploits-only    Show only vulnerabilities with known exploits
  --hide HIDDENVULN [HIDDENVULN ...]
                        Hide vulnerabilities of for example Adobe Flash Player
                        and Microsoft Edge
  -i IMPACTS [IMPACTS ...], --impact IMPACTS [IMPACTS ...]
                        Only display vulnerabilities with a given impact
  -s SEVERITIES [SEVERITIES ...], --severity SEVERITIES [SEVERITIES ...]
                        Only display vulnerabilities with a given severity
  -o [OUTPUTFILE], --output [OUTPUTFILE]
                        Store results in a file
  --muc-lookup           Hide vulnerabilities if installed hotfixes are listed
                        in the Microsoft Update Catalog as superseding
                        hotfixes for the original BulletinKB
  -h, --help            Show this help message and exit

examples:
  Download latest definitions
  wes.py --update
  wes.py -u

  Determine vulnerabilities
  wes.py systeminfo.txt
```

>>wes.py --update

```
F:\test\wesng>wes.py --update
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip2 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[*] Updating definitions
[*] Obtained definitions created at 20210607

F:\test\wesng>
```

Export SystemInfo into a txt file

>>systeminfo > systeminfo.txt

```
F:\test\wesng>systeminfo > systeminfo.txt

F:\test\wesng>
```

```
systeminfo - Notepad
File Edit Format View Help

Host Name:                GARRICK-LAPTOP
OS Name:                  Microsoft Windows 10 Home Single Language
OS Version:               10.0.19043 N/A Build 19043
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         dnamritesh@gmail.com
Registered Organization:
Product ID:                00327-35820-31051-AADEM
Original Install Date:     21-04-2021, 01:52:54 AM
System Boot Time:          08-06-2021, 10:03:08 PM
System Manufacturer:       Dell Inc.
System Model:              Inspiron 5570
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1600 Mhz
BIOS Version:              Dell Inc. 1.4.1, 24-12-2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:                \Device\HarddiskVolume6
System Locale:              en-us;English (United States)
Input Locale:               00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:      16,282 MB
Available Physical Memory:  6,993 MB
Virtual Memory: Max Size:  18,714 MB
Virtual Memory: Available: 5,785 MB
Virtual Memory: In Use:     12,929 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:               \\GARRICK-LAPTOP
Hotfix(s):                  13 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4534170
                           [03]: KB4537759
                           [04]: KB4542335
                           [05]: KB4545706
                           [06]: KB4557968
                           [07]: KB4562830
                           [08]: KB4577586
                           [09]: KB4580325

Ln 1, Col 1      100%  Windows (CRLF)  UTF-8
```

>>wes.py systeminfo.txt

```
Select Command Prompt
F:\test\wesng>systeminfo > systeminfo.txt
F:\test\wesng>wes.py systeminfo.txt
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip2 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitadmin/wesng/ )
[*] Parsing systeminfo output
[*] Operating System
  - Name: Windows 10 Version 20H2 for x64-based Systems
  - Generation: 10
  - Build: 19043
  - Version: 20H2
  - Architecture: x64-based
  - Installed hotfixes (11): KB5003254, KB4534170, KB4537759, KB4542335, KB4545706, KB4557968, KB4562830, KB4577586, KB4580325, KB4589212, KB5000736, KB5003173, KB5003242
[*] Loading definitions
  - Creation date of definitions: 20210607
[*] Determining missing patches
[*] Found vulnerabilities

Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a

Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a

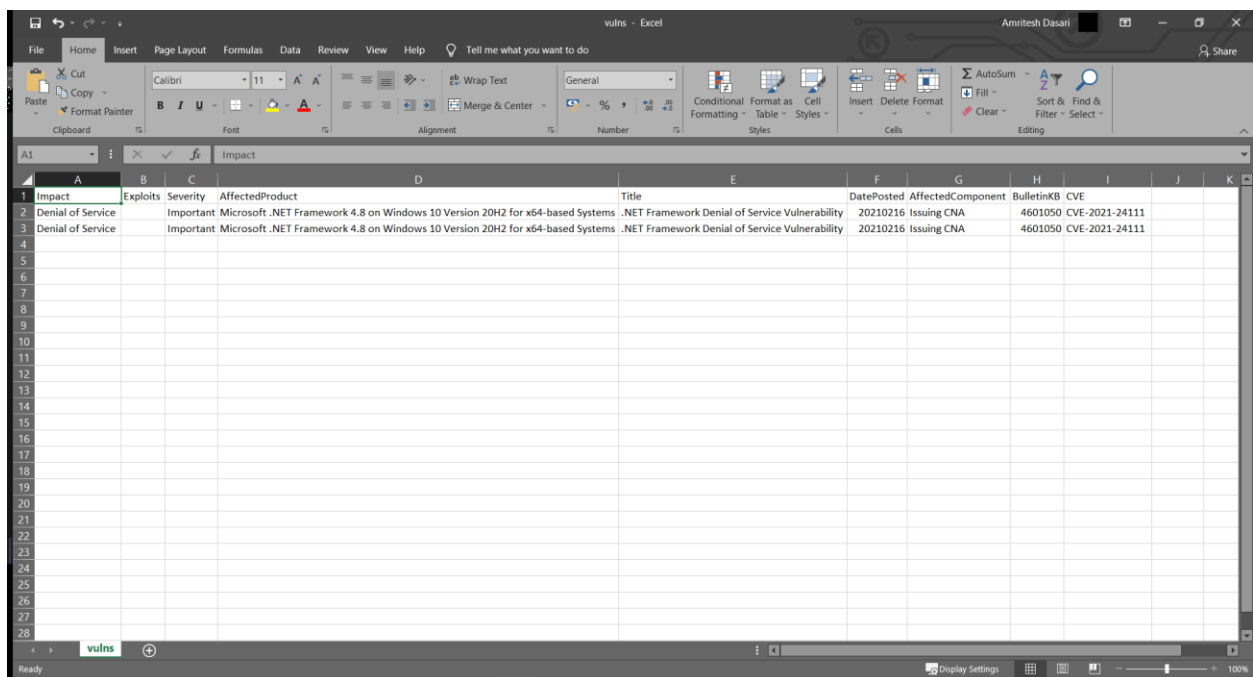
[*] Missing patches: 1
  - KB4601050: patches 2 vulnerabilities
[*] KB with the most recent release date
  - ID: KB4601050
  - Release date: 20210216
[*] Done. Displaying 2 of the 2 vulnerabilities found.

F:\test\wesng>
```

>>wes.py systeminfo.txt --output vulns.csv

```
F:\test\wesng>wes.py systeminfo.txt --output vulns.csv
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip2 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 10 Version 20H2 for x64-based Systems
  - Generation: 10
  - Build: 19043
  - Version: 20H2
  - Architecture: x64-based
  - Installed hotfixes (13): KB5003254, KB4534170, KB4537759, KB4542335, KB4545706, KB4557968, KB4562830, KB4577586, KB4580325, KB4589212, KB5000736, KB5003173, KB5003242
[+] Loading definitions
  - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
[+] Writing 2 results to vulns.csv
[+] Missing patches: 1
  - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
  - ID: KB4601050
  - Release date: 20210216
[+] Done. Saved 2 of the 2 vulnerabilities found.

F:\test\wesng>
```



Impact	Exploits	Severity	AffectedProduct	Title	DatePosted	AffectedComponent	BulletinKB	CVE
Denial of Service		Important	Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems	.NET Framework Denial of Service Vulnerability	20210216	Issuing CNA	4601050	CVE-2021-24111
Denial of Service		Important	Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems	.NET Framework Denial of Service Vulnerability	20210216	Issuing CNA	4601050	CVE-2021-24111