Secure Coding Lab
5th June, 2021

G.GAYATHRI
19BCN7034

1. Generating System Information in the sysinfo.txt file


```
Command Prompt                                                              —    □    ✕

Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>cd C:\wesng-master

C:\wesng-master>systeminfo > sysinfo.txt

C:\wesng-master>
```

The SystemInfo.txt file


```
sysinfo.txt - Notepad

File  Edit  Format  View  Help

Host Name:                  DESKTOP-7GDRFKM
OS Name:                    Microsoft Windows 10 Home
OS Version:                 10.0.19041 N/A Build 19041
OS Manufacturer:            Microsoft Corporation
OS Configuration:           Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:           user
Registered Organization:
Product ID:                 00326-10000-00000-AA051
Original Install Date:      17-11-2020, 14:29:25
System Boot Time:           12-06-2021, 09:13:08
System Manufacturer:        HP
System Model:               HP Pavilion Laptop 15-cc0xx
System Type:                x64-based PC
Processor(s):               1 Processor(s) Installed.
                            [01]: Intel64 Family 6 Model 142 Stepping 9 GenuineIntel ~2703 Mhz
BIOS Version:               Insyde F.10, 28-07-2017
Windows Directory:          C:\Windows
System Directory:           C:\Windows\system32
Boot Device:                \Device\HarddiskVolume7
```

2. Updating WES-NG with the latest database


```
C:\wesng-master>pip3 install chardet
Requirement already satisfied: chardet in c:\users\user\appdata\local\programs\python\python36\lib\site-packages (4.0.0)
WARNING: You are using pip version 21.0.1; however, version 21.1.2 is available.
You should consider upgrading via the 'c:\users\user\appdata\local\programs\python\python36\python.exe -m pip install --upgrade pip'
 command.

C:\wesng-master>wes.py --update
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210607

C:\wesng-master>
```

3. Checking for Vulnerabilities

```
Command Prompt                                                                    —   □   ×

C:\wesng-master>wes.py sysinfo.txt
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 (11): KB5003254, KB4561600, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities

Date: 20200714
CVE: CVE-2020-1346
KB: KB4566785
Title: Windows Modules Installer Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20200811
CVE: CVE-2020-1476
KB: KB4569745
Title: ASP.NET and .NET Elevation of Privilege Vulnerability
Affected product: Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20200811
CVE: CVE-2020-1046
KB: KB4569745
Title: .NET Framework Remote Code Execution Vulnerability
Affected product: Microsoft .NET Framework 3.5 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
```

```
Command Prompt                                                                    —   □   ×
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20210511
CVE: CVE-2021-31208
KB: KB5003173
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

[+] Missing patches: 4
    - KB5003173: patches 50 vulnerabilities
    - KB4569745: patches 2 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
    - KB4566785: patches 1 vulnerability
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 55 of the 55 vulnerabilities found.

C:\wesng-master>
```

The vulnerabilities can be prevented by downloading the KB5003173, KB4569745, KB4601050 and KB4566785 patches.

4. Patching

The patches are installed in our PC but due to some errors the tool WES-NG couldn't recognise it.

> **Quality Updates (5)**
>
> 2021-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)
> Successfully installed on 14-05-2021

So when we try to reinstall the same patches, we are not able to install them due to some errors from the OEM or simply Microsoft.
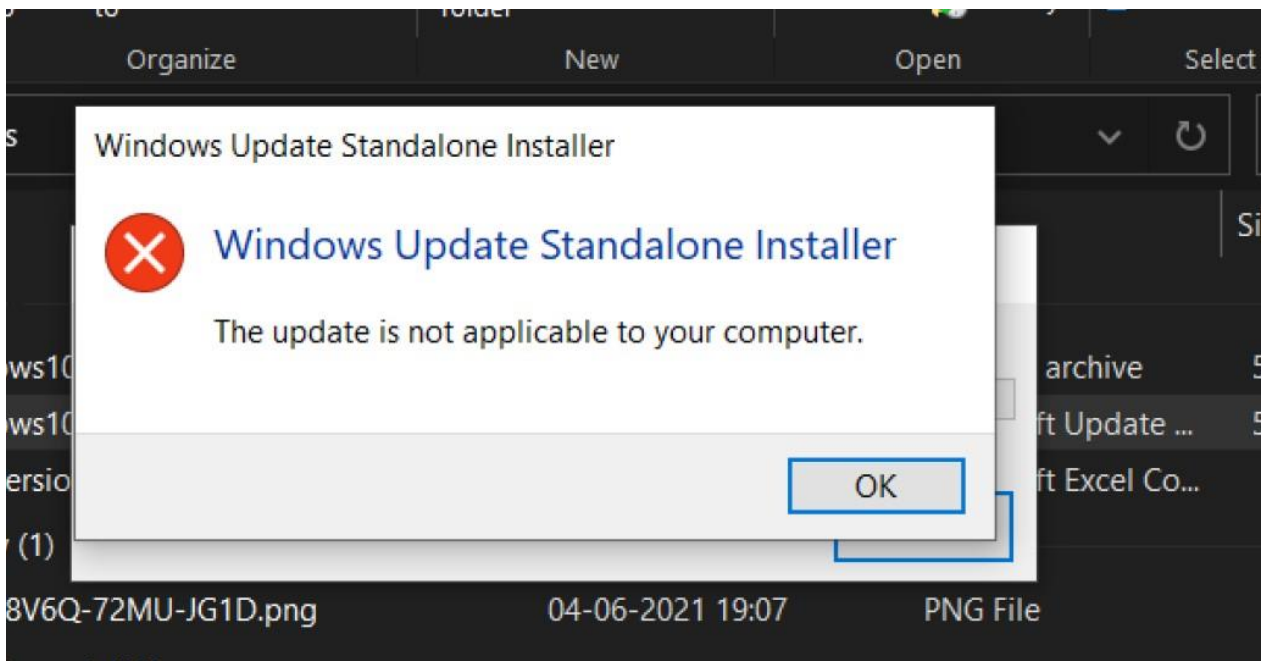
Hence we cannot install the patches to make the found vulnerability count '0'.

5. Another Way of finding dangerous vulnerabilities
We can also filter out the output in the tool WES-NG by adding display filters before scanning for vulnerabilities.

```
C:\wesng-master>wes.py -e sysinfo.txt --hide "Internet Explorer" Edge
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 (11): KB5003254, KB4561600, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found

C:\wesng-master>
```

Hence we get 0 vulnerabilities if we apply display filters. This shows that there aren't any major vulnerabilities that cannot be patched from updates.