

Secure Coding Lab - 13

Name: S V Girish Kumar

Reg. No: 18BCN7106

After installing the wesng from github.

```
cmd
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SATYAM>cd C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master

C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>python3 wes.py
Python was not found; run without arguments to install from the Microsoft Store, or disable this shortcut from Settings
> Manage App Execution Aliases.

C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>python wes.py
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 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
```

```
cmd

Download latest version of WES-NG
wes.py --update-wes

C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>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/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210530
```

```
cmd

C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>systeminfo > after_systeminfo.txt

C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>wes.py after_systeminfo.txt
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/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 10 Version 20H2 for x64-based Systems
  - Generation: 10
  - Build: 19042
  - Version: 20H2
  - Architecture: x64-based
  - Installed hotfixes (10): KB5003254, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5003214, KB5003503
[+] Loading definitions
  - Creation date of definitions: 20210530
[+] 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
```

```
cmd
Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 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 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

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

[+] Done. Displaying 52 of the 52 vulnerabilities found.
C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>
```

These are the vulnerabilities found in the machine. And the above-mentioned 50 vulnerabilities are patched in this report.

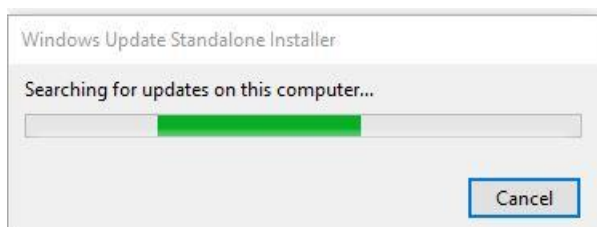
Microsoft Update Catalog

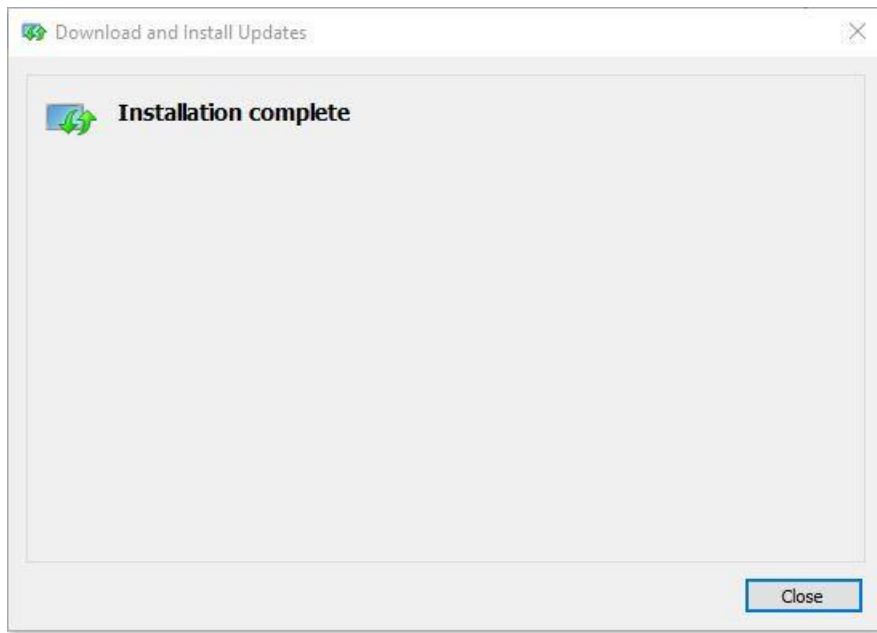
Search results for "KB5003173"

Updates: 1 - 22 of 22 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later, Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later, Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later, Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 2004 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 2004 for ARM64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows Server, version 20H2 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download

Downloaded the respective .msu file and started installing it.





Now running again the systeminfo and wes.py:

```
cmd
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.
C:\Users\SATYAM\Videos\SC_lab\wesng-master\wesng-master>
```

Now we can see 50 vulnerabilities are patched up and only 2 left. We can do similarly for them to patch up.