



CSE-2010 Secure Coding Lab-13

Name :- Amritmoy Pain

Reg. No. :- 18BCE7344

Windows exploit suggerster:

This is a tool that helps you to identify the vulnerability in your naïve windows system.

Double click on the setup.py to setup windows exploit suggerster. Now open command prompt do as follows

```
E:\College\SEM - 6\LABS\SECURE-CODING\wes ng\wesng-master\wesng-master>systeminfo > systeminfo_sc_demo.txt
E:\College\SEM - 6\LABS\SECURE-CODING\wes ng\wesng-master\wesng-master>wes.py systeminfo_sc_demo.txt
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: 19041
  - Version: 20H2
  - Architecture: x64-based
  - Installed hotfixes (9): KB5003254, KB4562830, KB4577586, KB4588125, KB4589212, KB4598481, KB5000736, KB5003214, KB
5003503
[+] Loading definitions
  - Creation date of definitions: 20210530
[+] Determining missing patches
[+] Found vulnerabilities
```

Pipe the systeminfo as a txt file to the wes.py and it will list all the vulnerabilities in the system. At last it will give you all the patches that are required to patch the vulnerabilities as below.

```
[+] 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.
```

Now go to the Microsoft catalog to download the required hotfixes I will be like below.

Microsoft Update Catalog

KB9008173

Search

1/27/2021

Search results for: 'KB9008173'

Updates 1 - 20 of 22 (page 1 of 1)

Previous / Next >

Title	Products	Classification	Last Updated	Version	Size	Download
KB9008173 Cumulative Update for Windows 10 Version 1713 for ARM64-based Systems (KB9008173)	Windows 10 version 1713 and later Windows Insider Pre-Release	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1713 for x86-based Systems (KB9008173)	Windows 10 version 1713 and later Windows Insider Pre-Release	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1713 for x86-based Systems (KB9008173)	Windows 10 version 1713 and later Windows Insider Pre-Release	Security Updates	3/14/2021	x64	295.0 KB	Download
KB9008173 Cumulative Update for Windows Server version 1809 for ARM-based Systems (KB9008173)	Windows Server version 1809 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1809 for ARM-based Systems (KB9008173)	Windows 10 version 1809 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB9008173)	Windows 10 version 1809 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB9008173)	Windows 10 version 1809 and later	Security Updates	3/14/2021	x64	294.0 KB	Download
KB9008173 Cumulative Update for Windows Server version 1909 for ARM64-based Systems (KB9008173)	Windows Server version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1909 for ARM64-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows Server version 1909 for x86-based Systems (KB9008173)	Windows Server version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1909 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 1909 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	294.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB9008173)	Windows Server version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	294.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	313.0 KB	Download
KB9008173 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB9008173)	Windows 10 version 1909 and later	Security Updates	3/14/2021	x64	294.0 KB	Download

Download the appropriate hotfixes for your pc type **winver** in start to get the version of the pc you are using. Download your hotfixes and fix your vulnerabilities.



```
C:\Windows\System32\rundll32.exe
```

Severity: Important

Impact: Security Feature Bypass

Exploit n/a

Date 20210511

CVE CVE-2021-31208

KB KB5003173

Title: Windows Container Manager Service Elevation of Privilege Vulnerability

Affected products: Windows 10 Version 20H2 To x64-based Systems Affected component: Trusted Engine UI

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 products: Windows 10 Version 20H2 To x64-based Systems Affected component: Trusted Engine UI

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 products: Windows 10 Version 20H2 To x64-based Systems Affected component: Trusted Engine UI

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 products: Windows 10 Version 20H2 To x64-based Systems Affected component: Trusted Engine UI

Severity: Critical

Impact: Remote code Execution

Eypla it n/a

[+] Missing patches: 2

- KB5003173 pat r he s 50 vulne rabi 1it ie s

- KB4601050 pat r he s 2 vulne rabi 1it ie s

[+ KB tvdth the mo s l ne r ent ne1ease date

- ID KB500317 3

- Relea s e date 20210511

[+ d Done . D i s p let' ing 82 of the 82 vu lne ceb i l it ie s I ound .

