



---

## Secure Coding Lab-13

*Name :- SRESTH MAHENDRA*

*Reg. No. :- 18BCE7039*

*Windows exploit suggester:*

*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 suggester. 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): KB5001254, KB4562830, KB4577580, KB4580125, KB4580212, KB4508401, KB5000730, KB5003214, KB
5001503
[+] Loading definitions
  - Creation date of definitions: 20210510
[+] 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.*

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

Microsoft Update Catalog							
Search results for "KB5003173"							
Results 1 - 20 of 20 items 1 of 1							
Title	Products	Category	Last Updated	Version	Size	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later Windows Insider Pre-Release	Security Updates	8/16/2021	x/6	494.0 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later Windows Insider Pre-Release	Security Updates	8/16/2021	x/6	473.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later Windows Insider Pre-Release	Security Updates	8/16/2021	x/6	475.4 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows Server version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows Server version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows Server version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	Download	
2021-08 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 version 20H2 and later	Security Updates	8/16/2021	x/6	513.6 MB	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:\W\ndows\SysTe m32\r md exe

Severity: Important

Impact: Security Feature Bypass

Eypla it n/a

Date 20210511

CVE CVE-2021-31208

KB KB5003173

Title: Windows Container Manager Service Elevation of Privilege Vulnerability

ATTN ted produ t iTi ndo ys 10 Vension 20H2 To xñ4-based Sy s terns ATN ted r omponenI T s uEng C U

Severity: Important

Impact: Elevation of Privilege

Eypla it n/a

Date 20210511

CVE CVE-2021-31208

KB KB5003173

Title: Windows Container Manager Service Elevation of Privilege Vulnerability

ATTN ted produ t iTi ndo ys 10 Vension 20H2 To xñ4-based Sy s terns ATN ted r omponenI T s uEng C U

Severity: Important

Impact: Elevation of Privilege

Eypla it n/a

Date 20210511

CVE CVE-2021-28476

KB KB5003173

Tit1e Hype r-V Remote code Eyerut ion vv1nerabi lity

ATTected product: Windows 10 Version 20H2 To: x64-based Systems ATTected component: Ts  
uEng C U  
Severity: critical  
Impact: Remote code Execution  
Exploit: n/a

Date: 20210511

CWE: CWE-2021-28476

KB: KB5003173

Title: Hyper-V Remote code Execution vulnerability

ATTected product: Windows 10 Version 20H2 To: x64-based Systems ATTected component: Ts  
uEng C U  
Severity: critical  
Impact: Remote code Execution  
Exploit: n/a

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

[+ d' Done. Disabling 82 of the 82 vulnerabilities I found.