

SECURE CODING LAB13

SLOT: L23+L24

NAME: CH KARTHIKEYA VARMA

REG NUM: 19BCD7138

Windows exploit suggester:

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

Follow the link in github to download the files required..... <https://github.com/bitsadmin/wesng>

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: 19043
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (9): KB5003254, KB4562830, KB4577586, KB4580325, 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

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
2021-05 Cumulative Update for Windows 10 Version 20H2 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 20H2 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 20H2 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 20H2 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU; Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	618.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003173)	Windows 10 GDR-DU; Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5003173)	Windows 10 GDR-DU; Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 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.



Microsoft Windows

Version 21H1 (OS Build 19043.1023)

© Microsoft Corporation. All rights reserved.

The Windows 10 Home Single Language operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the [Microsoft Software License](#)

[Terms](#) to:

user name

org name

OK

C:\Windows\System32\cmd.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 product: Windows 10 Version 20H2 for x64-based Systems
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 20H2 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 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.

