Name : Jayanth Chennupati

Regn No: 18BCN7084

Lab : 12

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

```
:\College\SEM - 6\LABS\SECURE-CODING\wes ng\wesng-master\wesng-master>systeminfo > systeminfo_sc_demo.txt
:\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 2042 for x64-based Systems
   - Generation: 10
   - Build: 19843
    - 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.

osoft Update Catalog			k85000175			- 4
centh roughs for "XB9000113" lest 1 - 22 of 32 (page 1 of 1)						_O Previous) for
Tile	Products	Confesion	Last Updated	Meralam	Size	Desnisat
2001-85 Completive Undate for Windows 10 Nation 2015 for ARMIN based Senters, NESSELETS	Windows 10, version 1983 and late; Windows Inside Pre-Reloade	Security Updates	5/16/0001	15/6	619.3 MB	Download
2011-05 Cumulative Update for Windows '01 Senson 21911 for old-based Systems (KESEE171)	Windows 10, version 1903 and later/Mindows Inside Pre-Belman	Security Updates	1/16/0001	19/8	111.0 MB	Download
3001-85 Cumulative Update for Windows 10 Nession 21911 for all6-based Systems 00050907/0	Windows 10, version 1983 and lates/Windows Insider Pre-Release	Security Updates	5/16/0001	10/9	2104 MB	Download
2021-85 Cumulative Update for Mindows Senso, version 2004 for e64-based Systems (KBSW0173)	Windows Server, version 1963 and later	Security Updates	5/10/2021	m/s	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Senson 2004 for s64-based Systems (000001173)	Windows 10, version 1903 and later	Security Updates	5/10/0001	19/0	STEE ME	Download
2021-05 Cumulative Update for Windows 10 Nesson 2004 for abli-based Systems (000002173)	Windows 10, version 1903 and later	Security Updates	5/10/9001	10/91	2104 MB	Download
2011-85 Comulative Update for Windows Server, version 2004 for ARM64 based Sertems (KBSRD 170)	Windows Server, version 1903 and later	Security Updates	5/10/2021	10/6	6893 MB	Download
2011 05 Cumulative Update for Mindows 10 Service 2005 for ARM66 Sussel Systems (085001111)	Windows 10, version 1903 and later	Security Updates	1/10/0001	n/a	619/3 MB	Download
3011-05 Cumulative Update for Windows Server, renson 3040 for edit-based Systems (100000115)	Windows Server, version 1903 and later	Security Updates	5/10/0001	19/9	21236 MB	Download
2001-85 Comulative Update for Windows 18 femion 2012 for s64-based Systems (KBSBD175)	Windows 10, version 1983 and later	Security Updates	5/10/2021	10/6	57256 MB	Download
2011-05 Comulative Update for Mindows 10 Service 2010 for old Search Spitems (CESSETTS)	Windows 10, version 1903 and later	Security Updates	5/10/0001	n/a	2104 MB	Download
2011-05 Cumulative Update for Windows Server, renson 2010 for MRMM-based Systems (KBSSSSTT):	Windows Server, version 1953 and later	Security Updates	5/10/2021	19/81	619/3 (48)	Download
2011-85 Cumulative Update for Windows 10 fersion 2012 for ARM64-based Systems 3005803 1735	Windows 10, version 1983 and later	Security Updates	5/10/2021	10/9	689.3 MB	Download
2001-05 Dynamic Cumulative Update for Windows 10 Version 2 II-II for ARM64 based Systems (88)0001113)	Windows 10 00th DUMindows Inside the Release	Security Updates	5/16/2021	10/10	6163 MB	Download
2011-05 Dynamic Cumulative Option for Windows 10 Version 219-0 for 469 based Systems (000001173)	Windows 10 GOR-DUSKindows Inside: Fire-Rateaux	Security Updates	5/16/2021	19/31	271.5 MB	Download
2011-85 Dynamic Cumulative Update for Windows 10 Version 219-9 for 486-based Systems X85003 (TX)	Windows 10 904-0U/Windows halder Pre-Release	Security Updates	5/16/2021	10/9	35919 MD	Download
2001-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x64-based Systems (HSS0061TS)	Windows 10 608-0U	Security Updates	5/10/2021	m/s	571.5 MB	Download
2011-01 Dynamic Cumulative Option for Windows 10 Version 2004 for alth-based Systems (60000111)	Windows 10 GDR-DU	Security Updates	1/10/0001	19/01	3868 MB	Download
2011-05 Dynamic Cumulative Opdate for Windows 10 Version 2004 for MRMSH based Systems (NSS000173)	Windows 10 GOR-DU	Security Updates	5/10/2001	10/9	6163 MB	Download
2011-95 Dynamic Cumulative Update for Windows 10 Version 2010 for x64-based Systems 3093001173)	Windows 10-008-0U	Security Updates	5/10/2021	m/e	571.5 MB	Download
2011-01 Dynamic Cumulative Update for Windows 10 Version 2010 for all Flowed Systems (000001110)	Windows 10 GDR-DU	Security Updates	1/10/0001	19/81	3068 MB	Download
2021-65 Dynamic Cumulative Option for Windows 10 Venior 201-0 for ARMA-based Systems 8050001731	Windows 10:908-8U	Security Updates	5/10/2021	10/9	6103 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.

About Windows



Microsoft Windows

Version 21H1 (DS Build 19043.1023)

© Microseft 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 cauntries/regions.

This product is licensed under the <u>Microsoft Software License</u> <u>Terms</u> 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

