

**Lab experiment – Automated Vulnerability Analysis and Patch Management
Experiment and Analysis**

- Deploy Windows Exploit Suggester - Next Generation (WES-NG)
- Obtain the system information and check for any reported vulnerabilities.
- If any vulnerabilities reported, apply the patch and make your system safe.
- Submit the auto-generated report using pwndoc. Happy

Learning!!!

EXPERIMENT

Step 1: Clone the following repository link to desktop Link:

<https://github.com/bitsadmin/wesng>

While cloning we can choose the destination folder to save this zip file.

Step 2: Get the System info by running the Systeminfo.exe and store the data in systeminfo.txt

Use the following commands and them in command prompt to get system info

System info > systeminfo.txt

notepad systeminfo.txt

The systeminfo.txt file contains the data related to system specifications, Hotfix, network cards and etc.

```
systeminfo - Notepad
File Edit Format View Help

Host Name:                DESKTOP-2TF9KQG
OS Name:                  Microsoft Windows 10 Home
OS Version:               10.0.19042 N/A Build 19042
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Lenovo
Registered Organization:
Product ID:                [REDACTED]
Original Install Date:     3/25/2021, 8:14:59 PM
System Boot Time:         6/5/2021, 8:28:51 AM
System Manufacturer:      LENOVO
System Model:              80TL
System Type:              x64-based PC

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

BEFORE PATCHING

Step 3:

Run the setup.py Then see update the wes.py to the latest version And then run the wes.py file for the systeminfo.txt file We will get the details of the vulnerabilities along with the appropriate patch.

```
C:\Users\Lenovo\Documents\wesng>wes.py --update
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[*] Updating definitions
[*] Obtained definitions created at 20210530

C:\Users\Lenovo\Documents\wesng>wes.py C:\Windows\System32\systeminfo.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: 19042
- Version: 20H2
- Architecture: x64-based
- Installed hotfixes (5): KB4601554, KB4562830, KB4580325, KB5003173, KB5003242
[*] 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

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
```

Missing patch

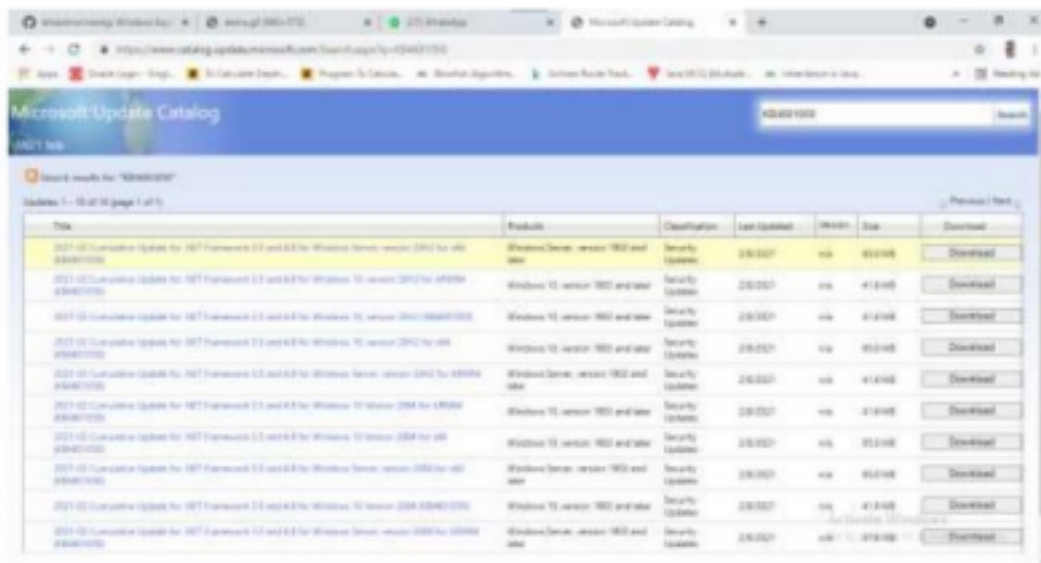
is KB4601050

Vulnerability: CVE-2021-24111

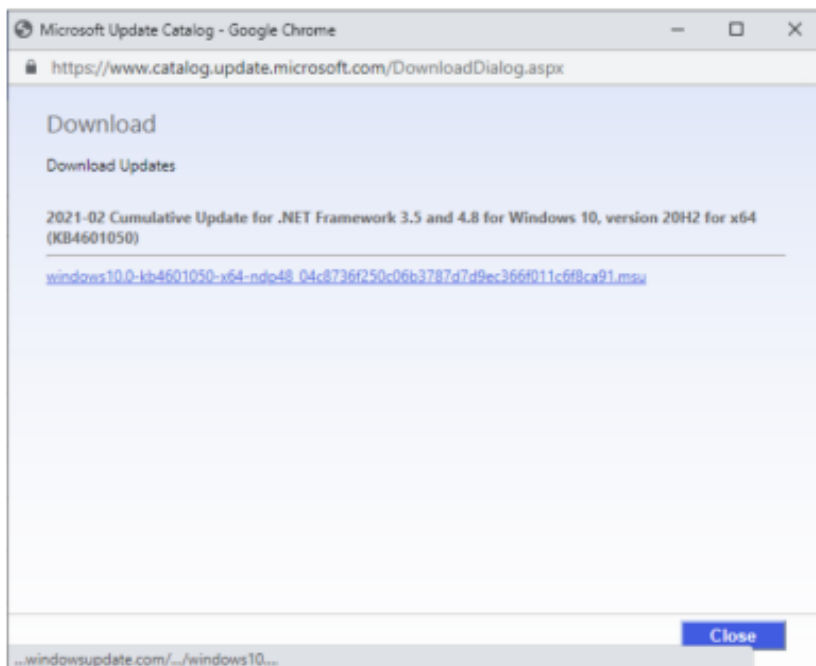
Description: .NET framework DOS (Denial of Service) Patch count required: 1

AFTER PATCH

Find the missing patch from the windows catalog and install it. Select the appropriate patch which is suitable for the system version and download it.



While clicking download we get a dialog box like this



We can also patch it by the searching on basis of vulnerability. If the missing patch is already downloaded then it gets updated and doesn't appear while running the test again. While running the test we noticed there is a missing patch

```
[+] 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.
```

This might be an OEM error and Microsoft hasn't resolved it yet.

```
C:\Users\Lenovo\Documents\wesng>wes.py -e sysinfo.txt --hide "Internet Explorer" Ed
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 (5): KB4601554, KB4562830, KB4580325, KB5003173, KB5003242
[+] Loading definitions
- Creation date of definitions: 20210530
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found

C:\Users\Lenovo\Documents\wesng>
```

We can use this command to find any major vulnerabilities and the system doesn't have any major vulnerability.