**CSE 2010 SECURE CODING**

**LAB SLOT –L23+L24**

**LAB-13**

**NAME-**KOTI VEERA PRABHU SAI GANESH MAJETI

**REG. NUMBER-**19BCN7073

**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 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.**

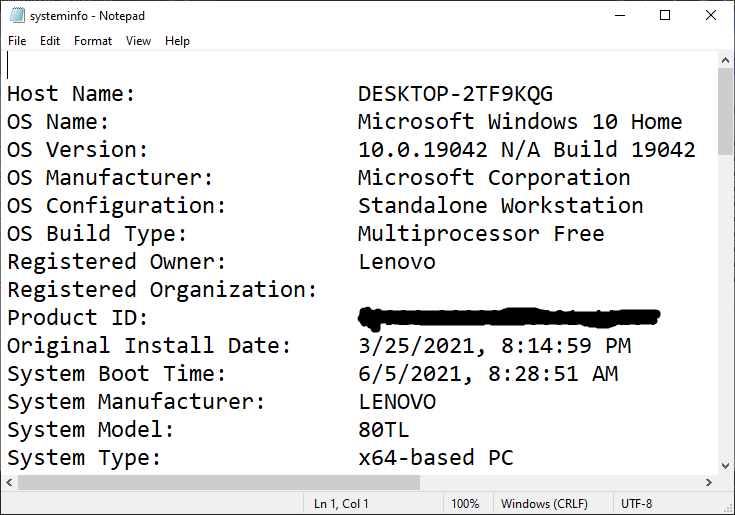
**Step 2: Get the System info by running the Systeminfo.exe and store the data in systeminfo.txt**

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

**systeminfo > systeminfo.txt**

**notepad systeminfo.txt**

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

****

**BEFORE PATCHING**

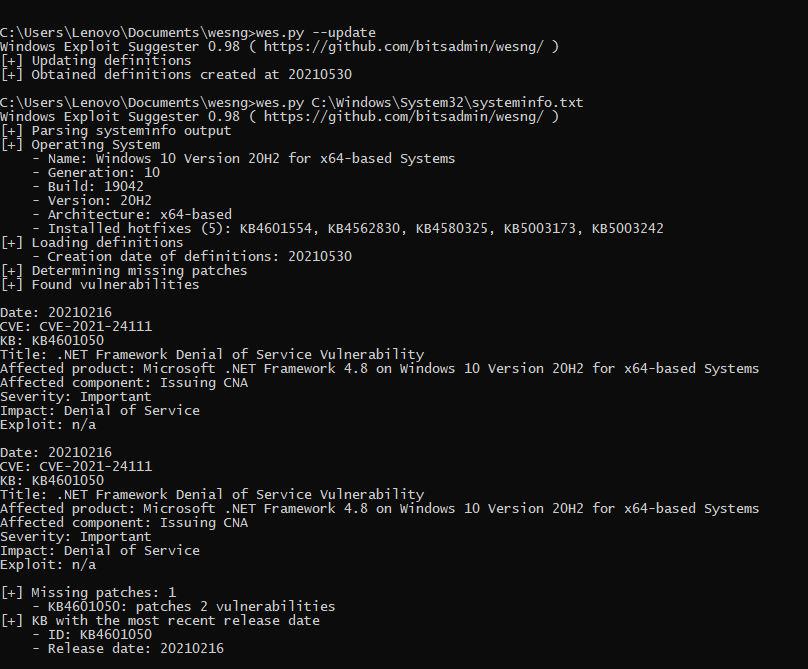
**Step 3:**

**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.**

****

**Missing patch is KB4601050**

**Vulnerability: CVE-2021-24111**

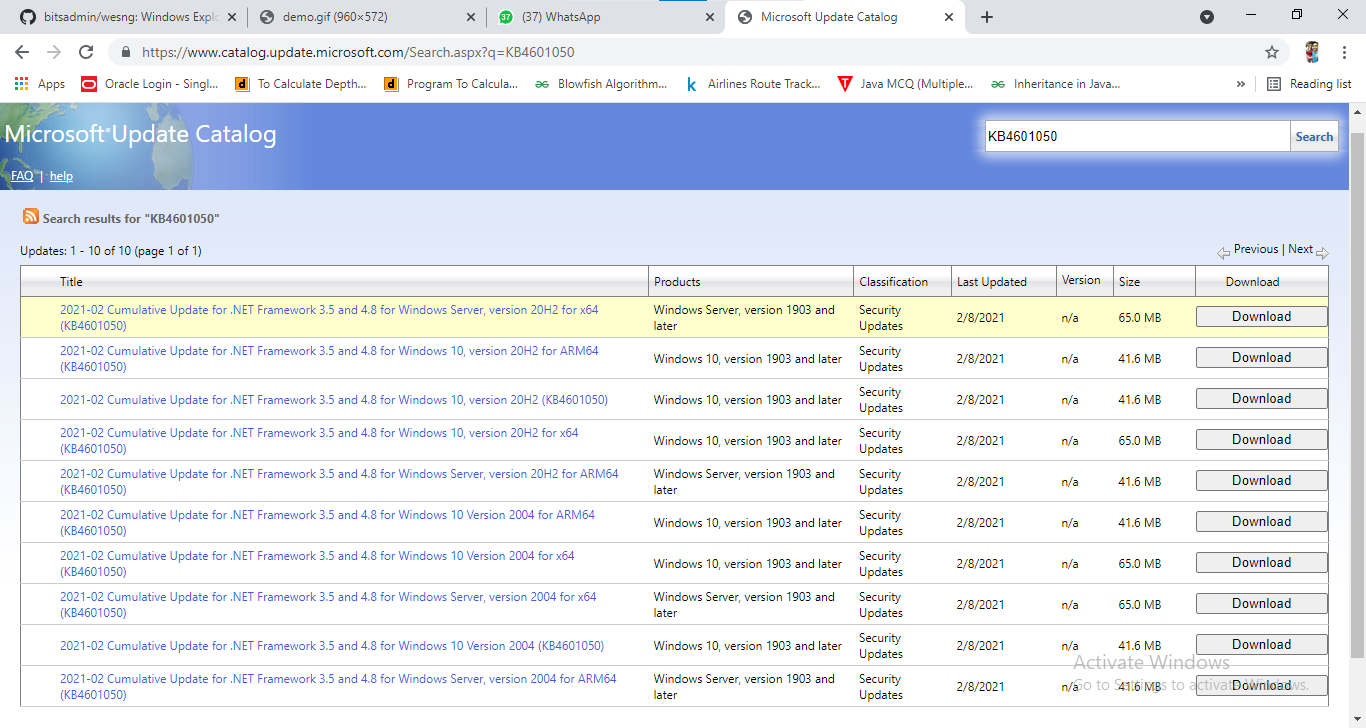
**Description: .NET framework DOS (Denial of Service)**

**Patch count required: 1**

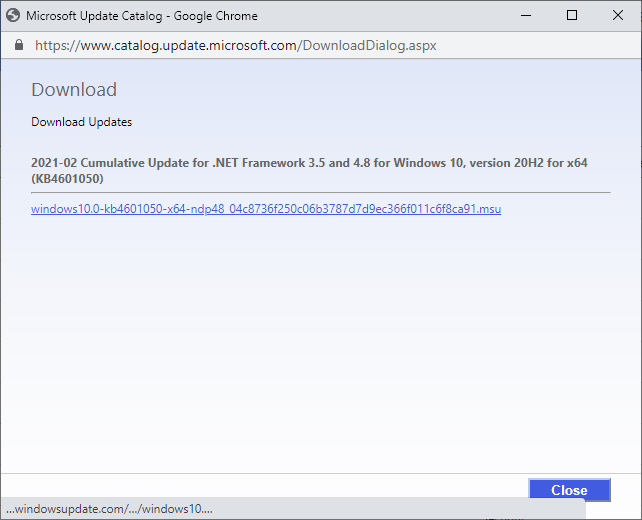
**AFTER PATCH**

**Find the missing patch from the windows catalogue and install it.**

**Select the appropriate patch which is suitable for the system version and download it.**

****

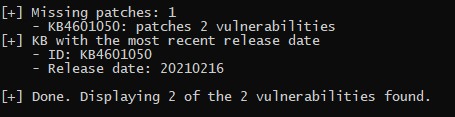
**While clicking download we get a dialog box like this**

****

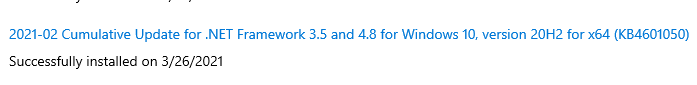
**We can also patch it by the searching on basis of vulnerability.**

**If the missing patch is already downloaded then it gets updated and doesn’t appear while running the test again.**

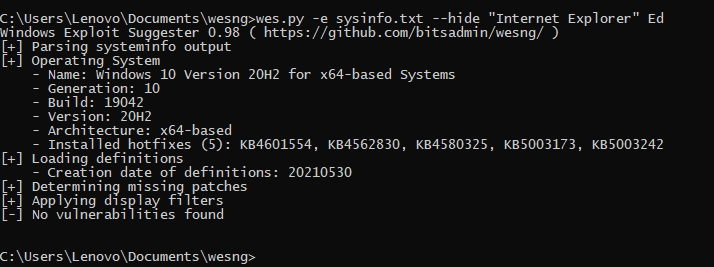
**While running the test we noticed there is a missing patch**

****

**But in the update history the patch is successfully installed and updated to the latest version**

****

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

****

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