CS559 Quantitative Security Fall 2023
Oluwatosin Falebita
Assignment 2a: Vulnerability Data Extraction and Analysis

In this assignment, I extracted vulnerability discovery data for two software products namely Windows 8, and Microsoft IIS HTTP Server from the National Vulnerability Database (NVD) database.

1. Specific Database, tools, and script.

a) Database: NVD
b) Specific tools: Windows 11 OS, Visual Studio Code, Python 3.11.4, and Microsoft Excel 2019.
c) Script: vulpullpy.py

Steps taken:

a. Download the required NVD database from 2002 to 2022 through this link https://nvd.nist.gov/vuln/data-feeds to a folder named nvd.
b. Extract the zip files into a new folder named json_data.
c. Place the vulpullpy.py into the same directory as the json_data.
d. Set the values of myText1 and myText2 fields to Windows 8 and Microsoft ISS respectively and also update the dataDir to the path of json_data/.
e. Include encoding='utf-8' on line 50 so that the script can read the JSON file format.
f. Run the vulpullpy.py script using Visual Studio code.
g. Two CSV (win8.csv and MSiis) and JSON two (win8.json and MSiis.json) files will be generated, these CSV files consist of Dates and Accum_CVEs columns, which were used to plot graphs.
h. The NVD website was used to search for recent vulnerabilities in Windows 8 and Microsoft ISS HTTP servers to get two vulnerabilities for each product.

2. Two most recent vulnerabilities in Windows 8 and Microsoft ISS HTTP servers.

Windows 8	Microsoft ISS HTTP servers
CVE-2023-32477	CVE-2022-45141
CVE-2023-40596	CVE-2021-37851

2.1 What is the name of the vulnerability in CVE format (e.g., CVE-2022-35722), and what it does? What are the CVSS Base Score and CVSS Temporal Score?

Windows 8

1. CVE format - CVE-2023-32477
   What it does: it affects Dell Common Event Enabler 8.9.8.2 for Windows and prior, it contains an improper access control vulnerability. A local low-privileged malicious user may potentially exploit this vulnerability to gain elevated privileges.
   CVSS Base Score: 7.8 (High)
   CVSS Temporal Score: Null

2. CVE format - CVE-2023-40596
   What it does: In Splunk Enterprise versions earlier than 8.2.12, 9.0.6, and 9.1.1, a dynamic link library (DLL) that ships with Splunk Enterprise references an insecure path for the OPENSSLDIR build definition. An attacker can abuse this reference and subsequently install malicious code to achieve privilege escalation on the Windows machine.
   CVSS Base Score: 8.8 (High)
   CVSS Temporal Score: Null

Microsoft ISS HTTP servers

1. CVE format - CVE-2022-45141
   What it does: Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96).
   CVSS Base Score: 9.8 (Critical)
   CVSS Temporal Score: Null

2. CVE format - CVE-2021-37851
   What it does: Local privilege escalation in Windows products of ESET allows user who is logged into the system to exploit repair feature of the installer to run malicious code with higher privileges.
   CVSS Base Score: 7.8 (High)
   CVSS Temporal Score: Null

2.2

Windows 8 - CVE-2023-32477

Date Published: 09/29/2023
Date Patched: 09/29/2023
Exploit for the vulnerability: Windows CEE versions prior to CEE 8.9.9.0
Solution for this vulnerability: Install CEE for Windows in the default location (Program Files folder). Do not install CEE in a custom folder.
Other products affected: Null

Windows 8 - CVE-2023-40596

Date Published: 2023-08-30
Date Patched: 2023-08-30
Exploit for the vulnerability:
Solution for this vulnerability: Restrict the permissions of the user that runs the splunkd process to core functionality.
Other products affected: Splunk Enterprise 8.2, Splunk Web 8.2.0 to 8.2.11, 8.2.12.

Microsoft ISS HTTP Servers - CVE-2022-45141

Date Published 03/06/2023
Date Patched: 09/17/2023

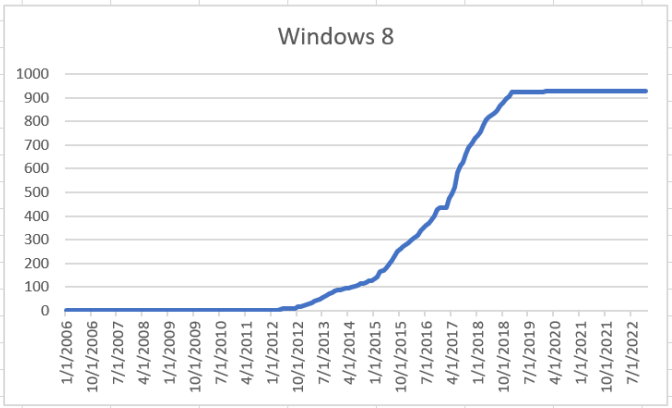
Exploit for the vulnerability: Samba Active Directory DCs
Solution for this vulnerability: Patch Availability.
Other products affected: Null

Microsoft ISS HTTP Servers - CVE-2021-37851

Date Published: 05/11/2022
Date Patched: 05/19/2022
Exploit for the vulnerability: ESET product for Windows
Solution for this vulnerability: ESET released an update of the Antivirus and antispyware scanner module to cover these vulnerabilities in already installed products, which was distributed automatically. ESET also released fixed builds of its products for Windows.
Other products affected: ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium versions from 11.2.

Windows 8 Vulnerability graph

Date	Accum_CVEs
1/1/2006	0
2/1/2006	0
3/1/2006	0
4/1/2006	0
5/1/2006	0
6/1/2006	0
7/1/2006	2
8/1/2006	2
9/1/2006	2
10/1/2006	2
11/1/2006	2
12/1/2006	2
1/1/2007	2
2/1/2007	2
3/1/2007	2
4/1/2007	3
5/1/2007	3
6/1/2007	3
7/1/2007	3
8/1/2007	3



Microsoft ISS HTTP Servers Vulnerability graph

Date	Accum_CVEs
1/1/1999	1
2/1/1999	1
3/1/1999	1
4/1/1999	1
5/1/1999	1
6/1/1999	1
7/1/1999	1
8/1/1999	1
9/1/1999	1
10/1/1999	1
11/1/1999	1
12/1/1999	1
1/1/2000	1
2/1/2000	1
3/1/2000	1
4/1/2000	1
5/1/2000	2