

My Windows 10 PC

# VULNERABILITY REPORT

SUNDAY, JUNE 13, 2021



---

**MODIFICATIONS HISTORY**

Version	Date	Author	Description
1.0	13/06/2021	Niharika Viswanadhuni	Initial Version

---

## TABLE OF CONTENTS

1.	General Information	4
1.1	Scope	4
1.2	Organisation	4
2.	Executive Summary	5
3.	Technical Details	6
3.1	Title	6
4.	Vulnerabilities summary	8

---

## GENERAL INFORMATION

---

### SCOPE

My Windows 10 PC has mandated us to perform security tests on the following scope:

- Exploiting Vulnerabilities in My Windows 10 PC

---

### ORGANISATION

The testing activities were performed between 13/06/2021 and 13/06/2021.

---

## EXECUTIVE SUMMARY

## VULNERABILITIES SUMMARY

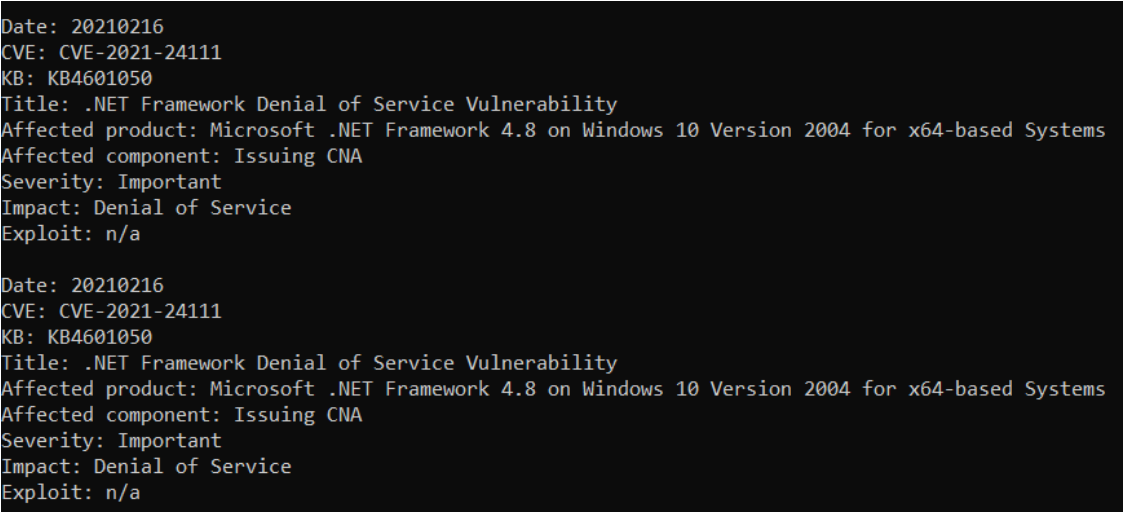
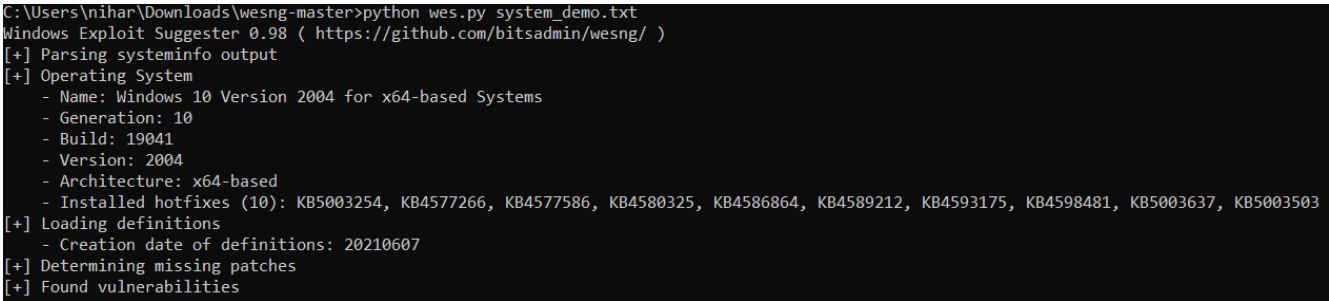
Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
Medium	VULN-001	.NET Framework Denial of Service Vulnerability	.Net Framework 4.8

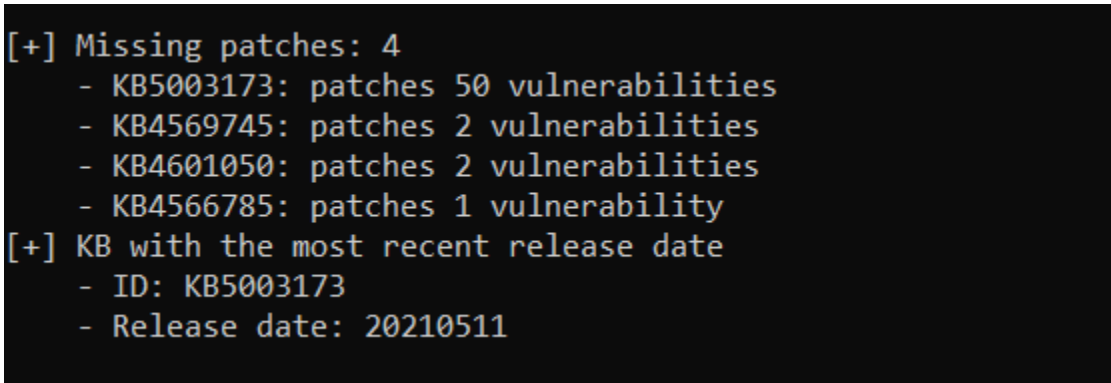
## TECHNICAL DETAILS

## .NET FRAMEWORK DENIAL OF SERVICE VULNERABILITY

CVSS SEVERITY	Medium	CVSSv3 SCORE	6.8
CVSSv3 CRITERIAS	Attack Vector : <b>Local</b> Attack Complexity : <b>Low</b> Required Privileges : <b>None</b> User Interaction : <b>None</b>	Scope : <b>Unchanged</b> Confidentiality : <b>Low</b> Integrity : <b>None</b> Availability : <b>High</b>	
AFFECTED SCOPE	.Net Framework 4.8		
DESCRIPTION	<p>C:\Users\nihar\Downloads\wesng-master&gt;python wes.py system_demo.txt            Windows Exploit Suggester 0.98 ( <a href="https://github.com/bitsadmin/wesng/">https://github.com/bitsadmin/wesng/</a> )            [+] Parsing systeminfo output            [+] Operating System              - Name: Windows 10 Version 2004 for x64-based Systems              - Generation: 10              - Build: 19041              - Version: 2004              - Architecture: x64-based              - Installed hotfixes (10): KB5003254, KB4577266, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503            [+] Loading definitions              - Creation date of definitions: 20210607            [+] Determining missing patches            [+] Found vulnerabilities            Date: 20210216            CVE: CVE-2021-24111            KB: KB4601050  <b>Title: .NET Framework Denial of Service Vulnerability</b>  <b>Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems</b>  <b>Affected component: Issuing CNA</b>  <b>Severity: Important</b>  <b>Impact: Denial of Service</b>  <b>Exploit: n/a</b>            Date: 20210216            CVE: CVE-2021-24111            KB: KB4601050  <b>Title: .NET Framework Denial of Service Vulnerability</b>  <b>Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems</b>  <b>Affected component: Issuing CNA</b>  <b>Severity: Important</b></p>		

	<p><b>Impact: Denial of Service</b>  <b>Exploit: n/a</b></p> <p>[+] Missing patches: 4</p> <ul style="list-style-type: none"> <li>- KB5003173: patches 50 vulnerabilities</li> <li>- KB4569745: patches 2 vulnerabilities</li> <li>- KB4601050: patches 2 vulnerabilities</li> <li>- KB4566785: patches 1 vulnerability</li> </ul> <p>[+] KB with the most recent release date</p> <ul style="list-style-type: none"> <li>- ID: KB5003173</li> <li>- Release date: 20210511</li> </ul> <p>[+] Done. Displaying 55 of the 55 vulnerabilities found.</p>  <p>The screenshot shows the output of the Windows Exploit Suggester tool. It lists two identical vulnerability entries. Each entry includes the date (20210216), CVE ID (CVE-2021-24111), KB ID (KB4601050), title (.NET Framework Denial of Service Vulnerability), affected product (Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems), affected component (Issuing CNA), severity (Important), impact (Denial of Service), and exploit status (n/a).</p> <p>Image 1 – Screenshot (138).png</p>
OBSERVATION	<p>As we have used Windows Exploit Suggester to check the vulnerabilities of my Windows 10 machine, we found these Vulnerabilities.</p> <p>Now, we can observe that this can lead to DOS (Denial of Service) of .Net framework 4.8.</p>
<p><b>TEST DETAILS</b></p> <p>I have Installed the recommended KB4601050 update &amp; successfully patched the DOS .Net framework 4.8 vulnerability</p>  <p>The screenshot shows the output of the Windows Exploit Suggester tool after the system has been patched. It displays the operating system information (Windows 10 Version 2004 for x64-based Systems, Generation 10, Build 19041, Version 2004) and lists installed hotfixes (KB5003254, KB4577266, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503). It also shows the creation date of definitions (20210607) and confirms that no missing patches or vulnerabilities were found.</p> <p>Image 1 – Patched.JPG</p>	



REMEDIATION	<p>[+] Missing patches: 1</p> <ul style="list-style-type: none"><li>- <b>KB4601050: patches 2 vulnerabilities</b></li></ul> <p>[+] KB with the most recent release date</p> <ul style="list-style-type: none"><li>- <b>ID: KB4601050</b></li><li>- Release date: 20210511</li></ul> <p>We can install these KB4601050 &amp; KB4601554(replaced by KB4601050) updates. This will fix/patch these vulnerabilities in our respective machines.</p>  <p>The screenshot shows a Windows Update window with a black background and white text. It lists missing patches and their release dates. The text is as follows:</p> <pre>[+] Missing patches: 4 - KB5003173: patches 50 vulnerabilities - KB4569745: patches 2 vulnerabilities - KB4601050: patches 2 vulnerabilities - KB4566785: patches 1 vulnerability [+] KB with the most recent release date - ID: KB5003173 - Release date: 20210511</pre> <p>Image 1 – Screenshot (139).png</p>
REFERENCES	Windows Update