My Windows 10 PC

VULNERABILITY REPORT

MONDAY, JUNE 07, 2021





MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/12/2021	KARTHIK G	Initial Version



TABLE OF CONTENTS

General Information	4
Scope 4	
Organisation	2
Executive Summary	5
Vulnerabilities summary	е
Technical Details	7
.NET Framework Denial of Service Vulnerability	7



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 06/07/2021 and 06/07/2021.



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 :	Local	Scope :	Unchanged
	Attack Complexity :	Low	Confidentiality :	Low
	Required Privileges :	None	Integrity:	None
	User Interaction :	None	Availability :	High
AFFECTED SCOPE	.Net Framework 4.8			



DESCRIPTION

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: 10Build: 19043Version: 20H2
- Architecture: x64-based
- Installed hotfixes (11): KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864,
- $\mathsf{KB4589212},\,\mathsf{KB4598481},\,\mathsf{KB5000736},\,\mathsf{KB5003173},\,\mathsf{KB5003242}$
- [+] 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
- [+] Done. Displaying 2 of the 2 vulnerabilities found.

```
25 Select Windows PowerShell
PS C:\Users\JAVVADI\Downloads\Compressed\wesng-master> python wes.py vuln.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: 19043
- Version: 20H2
- Architecture: x64-based
- Installed hotfixes (11): KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5000736, KB50 03173, KB5003242

[+] Loading definitions
- Creation date of definitions: 20210530
```



OBSERVATION

As, we have used Windows Exploit Suggester to check the vulnerabilities of my Windows 10 machine, We have found these Vulnerabilities we can observe that this can lead to DOS (Denial of Service) of .Net framework 4.8.

TEST DETAILS

I have Installed the recommended KB4601050 update & successfully patched the DOS .Net framework4.8 vulnerability

```
PS C:\Users\JAVYADI\Downloads\compressed\wesng-master> python wes.py vuln.txt -p KB4601050
windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )

[+] Parsing systeminfo output
[+] Operating System
[+] Operating System
[-] Name: Windows 10 Version 20H2 for x64-based Systems
[-] Generation: 10
[-] Build: 19043
[-] Version: 20H2
[-] Architecture: x64-based
[-] Installed hotfixes (11): KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5000736, KB5003173, KB5003242
[-] Manually specified hotfixes (1): KB4601050
[-] Loading definitions
[-] Loading definitions: 20210530
[-] Determining missing patches
[-] No vulnerabilities found
```

Image 1 - Patched.JPG

REMEDIATION

- [+] Missing patches: 1
- KB4601050: patches 2 vulnerabilities
- [+] KB with the most recent release date
- ID: KB4601050
- Release date: 20210216

We can install This KB4601050 & KB4601554(replaced update of KB4601050) updates. This will fix/patch these vulnerabilities in our respective machine.

```
led Windows PoweShell

- Build: 19043

- Version: 20H2

- Architecture: x64-based

- Installed hotfixes (11): kB4601554, kB4562830, kB4570334, kB4577586, kB4580325, kB4586864, kB4589212, kB4598481, kB5000736, kB50

73, kB5003242

Loading definitions

- Creation date of definitions: 20210530

Determining missing patches

Found vulnerabilities
        e: 20210216

CVE-2021-24111

K84601050
e: .NET Framework Denial of Service Vulnerability
e: .NET Framework Denial of Service Vulnerability
cted product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
cted component: Issuing CNA
crity: Important
ct: Denial of Service
oit: n/a
    te: 20210216
E: CVE-2021-24111
E: KB4601050
Itie: .NET Framework Denial of Service Vulnerability
Fected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
Fected component: Issuing CNA
verity: Important
pact: Denial of Service
ploit: n/a
[+] Missing patches: 1

- KB4601050: patches 2 vulnerabilities

[+] KB with the most recent release date

- ID: KB4601050
 [+] Done. Displaying 2 of the 2 vulnerabilities found.
                                                                                           O 🗎 | 🧑 🔚 境 р 🗷 🥝
                                                                                                                                                                                                                                           (3) ^ № [2] № // (4)) ENG 15:54
```

Image 1 – Screenshot (139).png

REFERENCES

Windows Update