My Windows 10 PC

VULNERABILITY REPORT

MONDAY, JUNE 07, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/11/2021	AKASH P	Initial Version

TABLE OF CONTENTS

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.

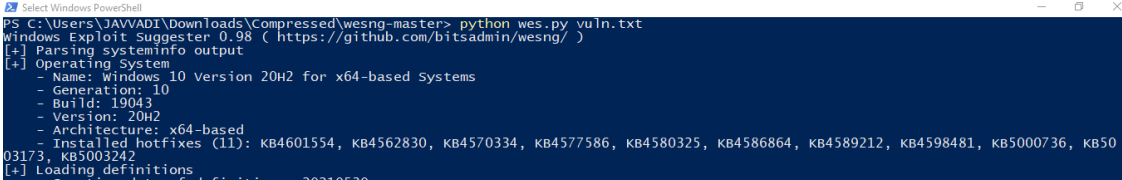# EXECUTIVE SUMMARY

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

```
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
[+] Determining missing patches
```

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\JAVVADI\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
    - 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
    - Creation date of 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.

```
    - Build: 19043
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (11): KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5000736, 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

[+] Done. Displaying 2 of the 2 vulnerabilities found.
PS C:\Users\JAVVADI\Downloads\Compressed\wesng-master>
```

Image 1 – Screenshot (139).png

REFERENCES	Windows Update