

N.Shanmukh - 18BCE7292

VULNERABILITY REPORT

THURSDAY, JUNE 010, 2021



MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/10/2021	N.SHANMUKH	Initial Version

TABLE OF CONTENTS

1.	General Information.....	4
1.1	Scope.....	4
1.2	Organisation.....	Error! Bookmark not defined.
2.	Executive Summary.....	5
3.	Technical Details.....	6
3.1	title.....	7
4.	Vulnerabilities summary.....	6

GENERAL INFORMATION

SCOPE

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

- Exploiting the open level Vulnerabilities in My Windows 10 PC

ORGANIZATION

The testing activities were performed between 06/07/2021 and 06/10/2021.

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 Attack Complexity : Low Required Privileges : None User Interaction : None Scope : Unchanged Confidentiality : Low Integrity : None Availability : High		
AFFECTED SCOPE	.Net Framework 4.8		
DESCRIPTION	<p>Windows Exploit Suggester 0.98 (https://github.com/bitsadmin/wesng/)</p> <p>[+] Parsing systeminfo output</p> <p>[+] Operating System</p> <ul style="list-style-type: none"> - 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 <p>[+] Loading definitions</p> <ul style="list-style-type: none"> - Creation date of definitions: 20210530 <p>[+] Determining missing patches</p> <p>[+] Found vulnerabilities</p> <p>Date: 20210216</p> <p>CVE: CVE-2021-24111</p> <p>KB: KB4601050</p> <p>Title: .NET Framework Denial of Service Vulnerability</p> <p>Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems</p> <p>Affected component: Issuing CNA</p> <p>Severity: Important</p> <p>Impact: Denial of Service</p> <p>Exploit: n/a</p> <p>Date: 20210216</p> <p>CVE: CVE-2021-24111</p> <p>KB: KB4601050</p> <p>Title: .NET Framework Denial of Service Vulnerability</p> <p>Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based</p>		

	<p>Systems</p> <p>Affected component: Issuing CNA</p> <p>Severity: Important</p> <p>Impact: Denial of Service</p> <p>Exploit: n/a</p> <p>[+] Missing patches: 1</p> <ul style="list-style-type: none"> - KB4601050: patches 2 vulnerabilities <p>[+] KB with the most recent release date</p> <ul style="list-style-type: none"> - ID: KB4601050 - Release date: 20210216 <p>[+] Done. Displaying 2 of the 2 vulnerabilities found.</p> <pre> 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, 03173, 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 </pre>
OBSERVATION	<p>As, I have used Windows Exploit Suggester to check the Vulnerabilities of my Windows 10 machine, I have found these Vulnerabilities.</p> <p>we can observe that this can lead to DOS (Denial of Service) attack of .Net framework 4.8.</p>
TEST DETAILS	<p>I have Installed the recommended KB4601050 update in windows power shell & had successfully patched the DOS .Net framework 4.8 Vulnerability</p> <pre> 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, KB503173, KB5003242 - Manually specified hotfixes (1): KB4601050 [+] Loading definitions - Creation date of definitions: 20210530 [+] Determining missing patches [-] No vulnerabilities found </pre>
REMEDIATION	<p>[+] Missing patches: 1</p> <ul style="list-style-type: none"> - KB4601050: patches 2 vulnerabilities

	<p>[+] KB with the most recent release date</p> <ul style="list-style-type: none">- ID: KB4601050- Release date: 20210216 <p>We can install This KB4601050 & KB4601554(replaced update of KB4601050) updates. This will fix/patch these vulnerabilities in our respective machine.</p> <pre>Select Windows PowerShell - Build: 19043 - Version: 20H2 - Architecture: x64-based - Installed hotfixes (11): KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5000736, 03173, 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</pre>
REFERENCES	Windows Update