|  |
| --- |
| vulnerabulity testing |
| Vulnerability Report |
| Tuesday, June 08, 2021 |



modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 06/08/2021 | SUMANTH tadiboina | 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

VITAP has mandated us to perform security tests on the following 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 06/08/2021.

# Executive Summary

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| Medium | VULN-001 | .NET Framework Denial of Service Vulnerability |  |

# 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** |  | | | | |
| **Description** | WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet  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 (10): KB5003254, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, 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.  image  Image 1 – Administrator\_ Command Prompt 06-06-2021 21\_27\_00.png | | | | |
| **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** | | | | | |
| **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. | | | | |
| **References** |  | | | | |