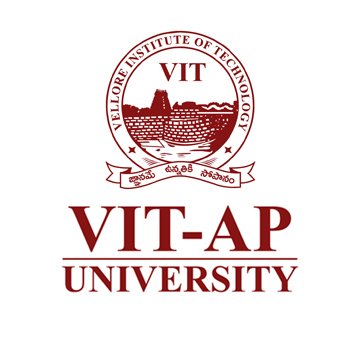
|  |
| --- |
| My PC Vuln |
| Vulnerability Report |
| Thursday, June 10, 2021 |



modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 06/10/2021 | R B CH S TARUN – 19BCN7122 | 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

VIT-AP has mandated us to perform security tests on the following scope:

* Testing Personal Computer Vulnerabilities using WES-NG

## Organisation

The testing activities were performed between 06/08/2021 and 06/11/2021.

# Executive Summary

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| Medium | VULN-001 | FINDING AND PATCHING Vuln's USING WES-NG | Affected product: net framework 4.8 on windows 10 version 20H2  ISSUSING CNA  Impact will be: DOS - DENIAL OF SERVICE |

# Technical Details

## FINDING AND PATCHING Vuln's USING WES-NG

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | Medium | | CVSSv3 Score | | 6.3 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **Low** | Confidentiality : | **Low** | |
| Required Privileges : | **Low** | Integrity : | **Low** | |
| User Interaction : | **None** | Availability : | **Low** | |
| **Affected scope** | Affected product: net framework 4.8 on windows 10 version 20H2  ISSUSING CNA  Impact will be: DOS - DENIAL OF SERVICE | | | | |
| **Description** | WES-NG is a tool based on the output of Windows' systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between Windows XP and Windows 10, including their Windows Server counterparts, is supported. | | | | |
| **Observation** | Now Let's see the detected vulnerabilities.  image  Image 1 – 5.PNG | | | | |
| **Test details**  The vulnerability detected is not patchable as the exact version of windows is not detected.  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4601050  image  Image 1 – image.png | | | | | |
| **Remediation** | Windows just need to release the patch for all the versions of their systems, so as of now it still remains un-patchable but as the risk is low its acceptable as of now. Impact will be denial of service.  image  Image 1 – 5.PNG | | | | |
| **References** | https://github.com/bitsadmin/wesng | | | | |