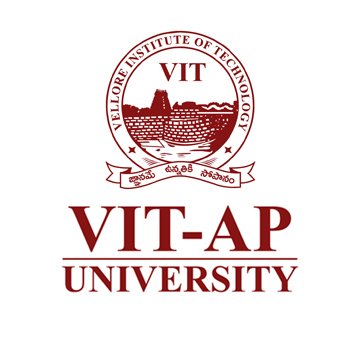
|  |
| --- |
| Buffer Overflow Vuln |
| Vulnerability Report |
| Thursday, June 10, 2021 |



modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 06/10/2021 | Gopi nandan,19bcn7056 | Working with memory vulnerabilities |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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:

* Exploiting the memory vulnerabilities.

## Organisation

The testing activities were performed between 06/09/2021 and 06/11/2021.

# Executive Summary

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| Medium | VULN-001 | Memory Vuln |  |

# Technical Details

## Memory Vuln

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVSS Severity** | **Medium** | | **CVSSv3 Score** | | **6.1** |
| **CVSSv3 criterias** | Attack Vector : | **Physical** | Scope : | **Changed** | |
| Attack Complexity : | **High** | Confidentiality : | **Low** | |
| Required Privileges : | **Low** | Integrity : | **High** | |
| User Interaction : | **Required** | Availability : | **Low** | |
| **Affected scope** |  | | | | |
| **Description** | **Buffer overflow** (or **buffer overrun**) occurs when the volume of data exceeds the storage capacity of the memory **buffer**. As a result, the program attempting to write the data to the **buffer** overwrites adjacent memory locations.  download the windows 7 in VMWare Workstation  Running the python script to generate payload.      Image 1produced a output file.PNG  run the script in command to get python script  After that running the python script the payload will be generated  After the payload is generated we have to open the stream ripper and we have to insert the payload into a intake search bar which posses vulnerability.  Then the stream ripper application crashes. | | | | |
| **Observation** | Image 1 – crashed.PNG | | | | |
| **Test details**    Image 1 – crashed.PNG | | | | | |
| **Remediation** | Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection. | | | | |
| **References** |  | | | | |