LAB - 12

# VULNERABILITY REPORT

SUNDAY, JUNE 09, 2021

CONFIDENTIAL

## MODIFICATIONS HISTORY

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 09/06/2021 | B.KRANTHI | Initial Version |
| | | | |
| | | | |
| | | | |



## TABLE OF CONTENTS

# General Information

## Scope

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

- This is for secure coding lab

## Organisation

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

# EXECUTIVE SUMMARY

## VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

| Risk | ID | Vulnerability | Affected Scope |
|---|---|---|---|
| High | IDX-002 | DDOS | |
| High | IDX-001 | Buffer overflow | |
| Medium | VULN-003 | Ransomware | |



## TECHNICAL DETAILS

### DDOS

| CVSS SEVERITY | High | CVSSv3 SCORE | 8.3 |
|---|---|---|---|
| CVSSv3 CRITERIAS | Attack Vector : **Network** Scope : **Changed** Attack Complexity : **High**<br>Confidentiality : **High**<br>Required Privileges : **None** Integrity : **High**<br>User Interaction : **Required** Availability : **High** | | |
| AFFECTED SCOPE | | | |
| DESCRIPTION | This is used to crash a website using multiple pinging | | |
| OBSERVATION | | | |
| TEST DETAILS | | | |
| REMEDIATION | | | |
| REFERENCES | | | |



### BUFFER OVERFLOW

| CVSS Severity | High | CVSSv3 Score | 7.6 |
|---|---|---|---|
| CVSSv3 criterias | Attack Vector : **Network** Scope : **Changed** Attack Complexity : **High**<br>Confidentiality : **High**<br>Required Privileges : **High** Integrity : **High**<br>User Interaction : **Required** Availability : **High** | | |
| Affected scope | | | |
| Description | This is a code level error normally made by humans due to the type casting errors. It lead to the crash of rocket ariane - 5. | | |
| Observation | This is done using steam ripper | | |
| Test details | | | |
| Remediation | | | |
| References | | | |



## Ransomware

| CVSS Severity | Medium | CVSSv3 Score | 6.2 |
|---|---|---|---|
| CVSSv3 criterias | Attack Vector : **Physical** Scope : **Unchanged** Attack Complexity : **High**<br>Confidentiality : **High**<br>Required Privileges : **Low** Integrity : **High**<br>User Interaction : **Required** Availability : **High** | | |
| Affected scope | | | |
| Description | This is used to infect the naive windows to get the ransom. | | |
| Observation | | | |
| Test details | | | |
| Remediation | | | |
| References | | | |