LAB - 12

VULNERABILITY REPORT

Wednesday, JUNE 09, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	09/06/2021	Varun Channa	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 9
4. Vulnerabilities summary 6

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**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**High**
	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**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	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**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	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				