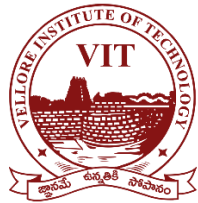


Secure Coding Lab

VULNERABILITY REPORT

WEDNESDAY, JUNE 09, 2021



VIT-AP

UNIVERSITY

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/09/2021	Sreenidhi Ganachari	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	11
4.	Vulnerabilities summary	6

GENERAL INFORMATION

SCOPE

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

- Vulnerabilities

ORGANISATION

The testing activities were performed between 05/15/2021 and 06/09/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-003	Buffer Overflow	
Medium	VULN-002	Memory Vulnerability	
Medium	IDX-002	Stack Overflow	

TECHNICAL DETAILS

BUFFER OVERFLOW

CVSS SEVERITY	High		CVSSv3 SCORE	8.1
CVSSv3 CRITERIAS	Attack Vector : Network	Scope : Changed	Attack Complexity : High	Confidentiality : High
	Required Privileges : Low	Integrity : Low	User Interaction : Required	Availability : High
AFFECTED SCOPE				
DESCRIPTION	Buffer Overflow vulnerability occurs when data more than required is entered into the buffer . The overflow leads to a system crash , but it gives opportunities to the attackers to manipulate the errors for malicious attacks.			
OBSERVATION	The observation in this buffer overflow is that it crashes the application			

TEST DETAILS

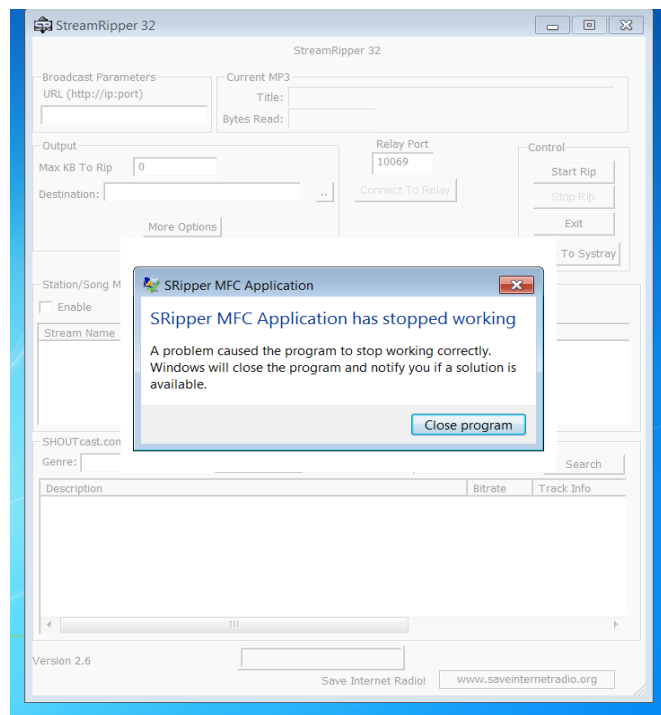


Image 1 – buffer.JPG

REMEDIATION	1) ASLR 2) DEP
REFERENCES	

MEMORY VULNERABILITY

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.7
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : Low Required Privileges : None User Interaction : Required	Scope : Changed Confidentiality : Low Integrity : Low Availability : High	
AFFECTED SCOPE			
DESCRIPTION	Buffer Overflow vulnerability occurs when data more than required is entered into the buffer . The overflow leads to a system crash , but it gives opportunities to the attackers to manipulate the errors for malicious attacks.		
OBSERVATION	The observation in this buffer overflow is that it crashes the application		

TEST DETAILS

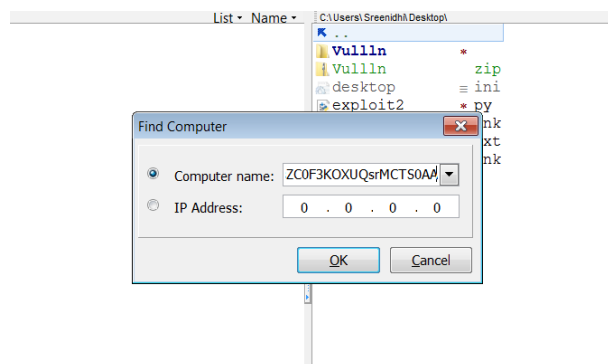
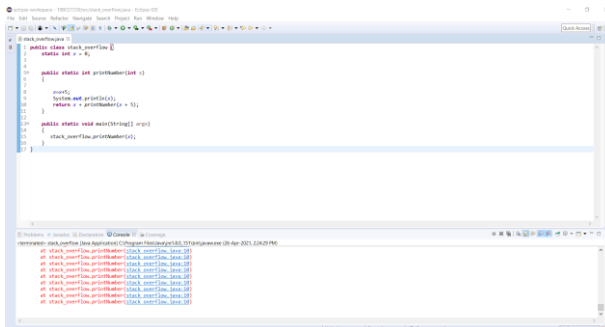


Image 2 – mem.JPG

After this the Frigate Application crashes to open the command prompt.

REMEDIATION	1. ASLR 2. DEP 3. SEHOP
REFERENCES	

STACK OVERFLOW

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.2
CVSSv3 CRITERIAS	Attack Vector : Local Attack Complexity : Low Required Privileges : None User Interaction : Required Scope : Unchanged Confidentiality : None Integrity : None Availability : High		
AFFECTED SCOPE			
DESCRIPTION	Stack Buffer Overflow occurs when a program writes to a memory address above it's fixed length and leads to the overflow .		
OBSERVATION	The program stops working and displays an error of stack overflow .		
TEST DETAILS	 <p>Image 3 – sta.JPG</p>		
REMEDIATION	1.ASLR - Randomization		
REFERENCES			

