VULNERABILITY REPORT

VIT-AP UNIVERSITY CONFIDENTIAL MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/17/2021	Sindhu Gurram	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 .....10 4.
Vulnerabilities summary 6

GENERAL INFORMATION

SCOPE

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

- Software Security

ORGANISATION

The testing activities were performed between 05/17/2021 and 05/31/2021.

EXECUTIVE SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-003	Shell code injection	
High	IDX-001	Buffer Overflow	
Medium	VULN-002	Denial of Service	

VIT-AP UNIVERSITY CONFIDENTIAL

TECHNICAL DETAILS

SHELL CODE INJECTION

CVSS SEVERITY	High	CVSSv3 SCORE	8.2
CVSSv3 CRITERIAS	Attack Vector : **Network** Scope : **Changed** Attack Complexity : **High** Confidentiality : **High** Required Privileges : **None** Integrity : **Low** User Interaction : **Required** Availability : **High**		
AFFECTED SCOPE			
DESCRIPTION	Summary: Shell code injection is a hacking technique where the hacker exploits vulnerable programs.The hacker infiltrates in to the vulnerable programs and makes it execute their own code.He injects code into a vulnerable computer program and change the course of execution.this injection leads to data loss,denial of access and even leads to inject the hosts takeover totally.		
OBSERVATION	We have already identified this vulnerability and can execute different malicious code and trigger with other applications like command prompt , control panel etc.		

TEST DETAILS

REMEDIATION	The attacker can steal data , identifying buffer flow vulnerability, Implementing ASLR and DEP.
REFERENCES	

CVSS SEVERITY	High	**CVSSv3 SCORE**	7.6
CVSSv3 CRITERIAS	Attack Vector : **Local** Scope : **Changed** Attack Complexity : **High** Confidentiality : **High** Required Privileges : **None** Integrity : **Low** User Interaction : **Required** Availability : **High**		
AFFECTED SCOPE			
DESCRIPTION	A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. It exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.		
OBSERVATION	We have observed that this buffer overflow can potentially crash an application and unknowingly allows command injection attacks.		

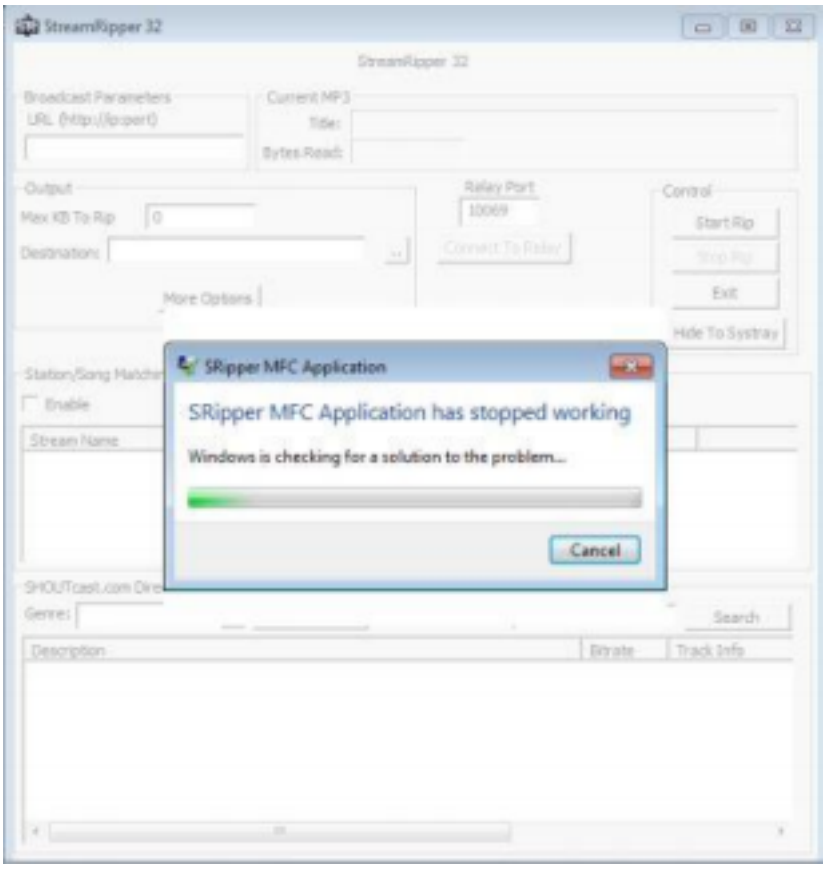
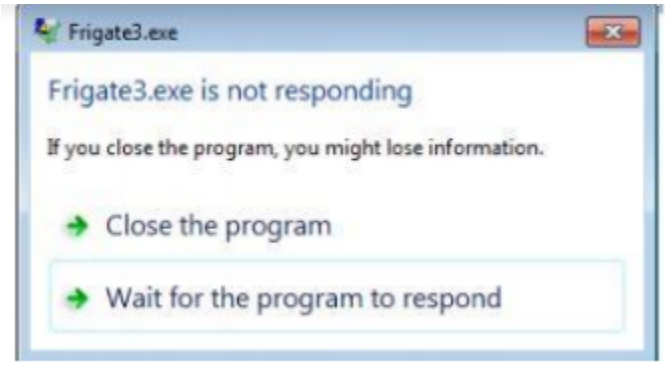
TEST DETAILS


Image 1 – doc.JPG	
REMEDIATION	1. Address space randomization (ASLR) 2. Data execution prevention (DEP) 3. Structured exception handler overwrite protection (SEHOP)
REFERENCES	

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.5

CVSSv3 CRITERIAS	Attack Vector : **Local** Scope : **Unchanged** Attack Complexity : **Low** Confidentiality : **None** Required Privileges : **None** Integrity : **None** User Interaction : **Required** Availability : **High**
AFFECTED SCOPE	
DESCRIPTION	The Denial of Service (DoS) attack is focused on making an software unavailable for the purpose it was designed. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses. I
OBSERVATION	We have observed that the software crashes immediately as a result of large string input due to Buffer overflow vulnerability. This could impact the availability of software
TEST DETAILS	 Image 2 – buff.JPG
REMEDIATION	!. Input Sanitization 2. Addressing Buffer Overflow
REFERENCES	