VULNERABILITY REPORT

VIT-AP
UNIVERSITY

MODIFICATIONS HISTORY

Version	**Date**	**Author**	**Description**
1.0	05/31/2021	Sai Sumedh Chittelu	Initial Version

TABLE OF CONTENTS

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

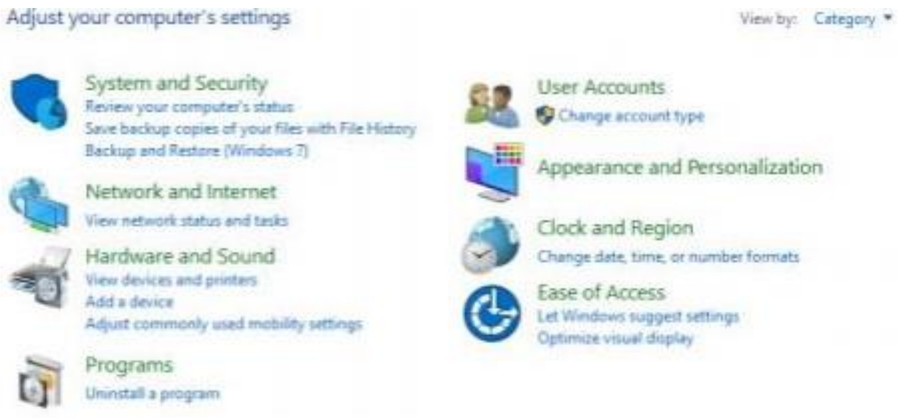
VULNERABILITY SUMMARY

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	

TECHNICAL DETAILS

SHELL CODE INJECTION

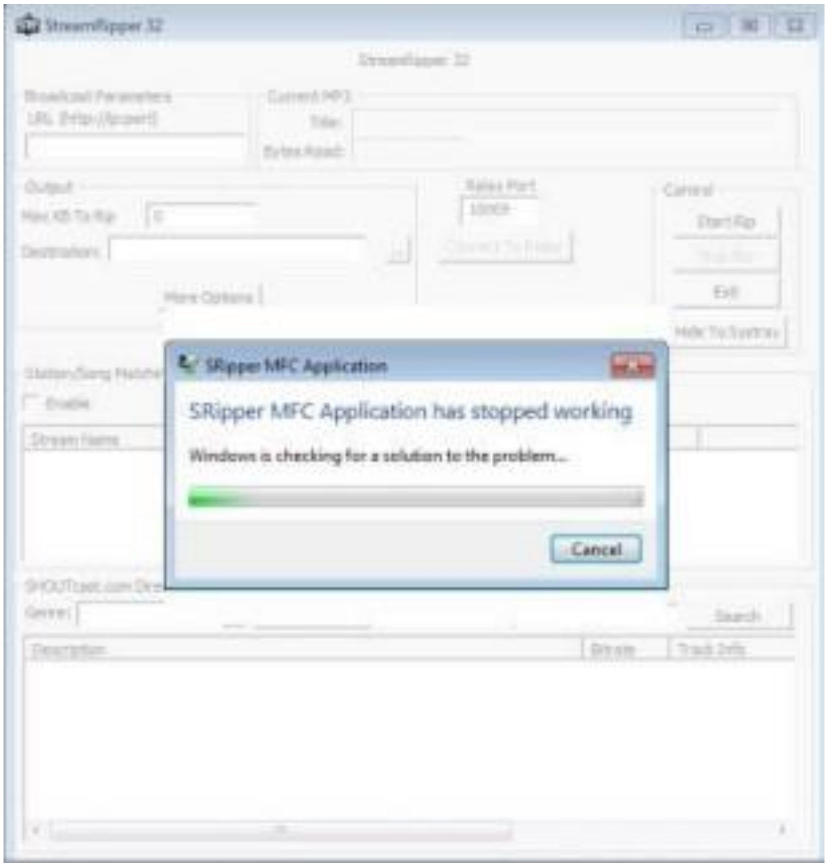
<table>
<tr><td><b>CVSS SEVERITY</b></td><td>High</td><td><b>CVSSv3 SCORE</b></td><td>8.2</td></tr>
<tr><td><b>CVSSv3 CRITERIAS</b></td><td colspan="3">Attack Vector : <b>Network</b> Scope : <b>Changed</b> Attack Complexity : <b>High</b>
Confidentiality : <b>High</b>
Required Privileges : <b>None</b> Integrity : <b>Low</b>
User Interaction : <b>Required</b> Availability : <b>High</b></td></tr>
<tr><td><b>AFFECTED SCOPE</b></td><td colspan="3"></td></tr>
<tr><td><b>DESCRIPTION</b></td><td colspan="3">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.</td></tr>
<tr><td><b>OBSERVATION</b></td><td colspan="3">We have already identified this vulnerability and can execute different malicious code and trigger with other applications like command prompt , control panel etc.</td></tr>
<tr><td colspan="4"><b>TEST DETAILS</b>

Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td><b>REMEDIATION</b></td><td colspan="3">The attacker can steal data , identifying buffer flow vulnerability, Implementing ASLR and DEP.</td></tr>
<tr><td><b>REFERENCES</b></td><td colspan="3"></td></tr>
</table>

Buffer Overflow

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

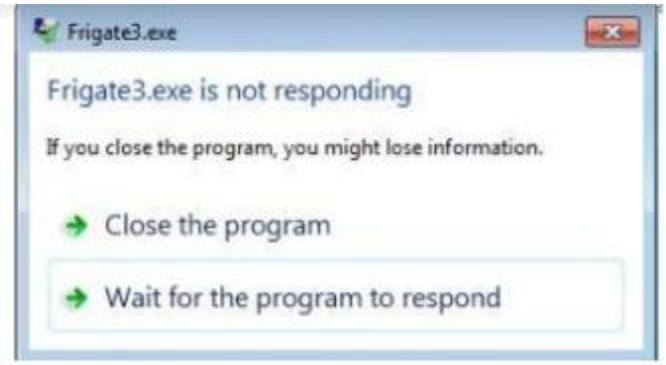


SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

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

Denial of Service

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	 Frigate3.exe is not responding If you close the program, you might lose information. Image 2 – buff.JPG		
Remediation	!. Input Sanitization 2. Addressing Buffer Overflow		
References			