

Stream Ripper 32 Frigate

# VULNERABILITY REPORT

Friday, JUNE 11, 2021



**VIT-AP**  
**UNIVERSITY**

---

**MODIFICATIONS HISTORY**

Version	Date	Author	Description
1.0	06/11/2021	Panwala Harshit Rakesh	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	6
4.	Vulnerabilities summary	8

---

## 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 06/11/2021 and 06/11/2021.

---

## EXECUTIVE SUMMARY{#SUMMARY}

---

## VULNERABILITIES 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{#FINDINGS}

### 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	<p>Shell code injection is a hacking technique where the hacker exploits vulnerable programs. The hacker infiltrates into the vulnerable programs and makes it execute their own code. he injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution.this injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.</p>			
OBSERVATION	<p>We have identified that this Vulnerability can execute different malicious code and can even trigger different applications including Command Prompt.</p>			

#### TEST DETAILS

```
Microsoft Windows [Version 10.0.19041.985]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>
```



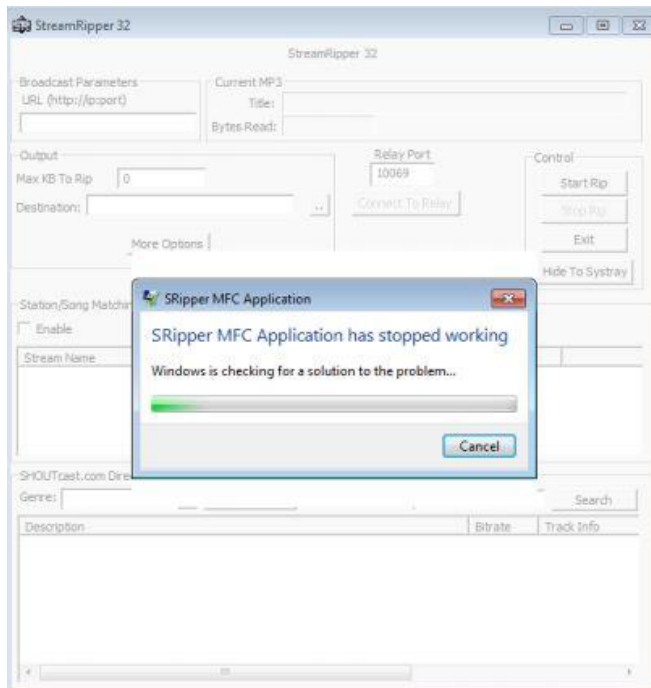
REMEDIATION	<ol style="list-style-type: none"><li>1. Addressing Buffer Overflow Vulnerability</li><li>2. Input Sanitization</li><li>3. Implementing ASLR, DEP, SEH</li></ol>
REFERENCES	



## BUFFER OVERFLOW

<b>CVSS SEVERITY</b>	<b>High</b>	<b>CVSSv3 SCORE</b>	<b>7.6</b>
<b>CVSSv3 CRITERIAS</b>	Attack Vector : <b>Local</b> Attack Complexity : <b>High</b> Required Privileges : <b>None</b> User Interaction : <b>Required</b>	Scope : <b>Changed</b> Confidentiality : <b>High</b> Integrity : <b>Low</b> Availability : <b>High</b>	
<b>AFFECTED SCOPE</b>			
<b>DESCRIPTION</b>	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.		
<b>OBSERVATION</b>	We have observed that this buffer overflow can potentially crash an application and unknowingly allows command injection attacks.		

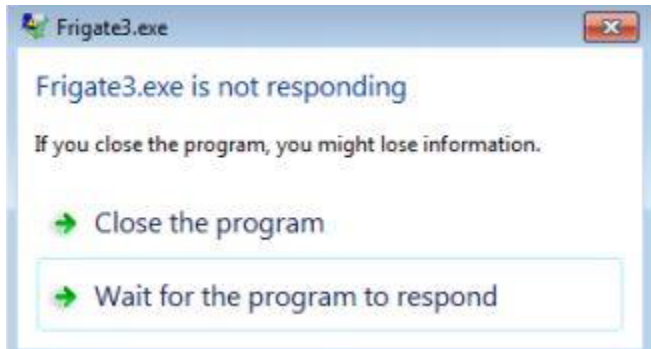
### TEST DETAILS



<b>REMEDIATION</b>	1. Address space randomization (ASLR) 2. Data execution prevention (DEP)
--------------------	---

	3. Structured exception handler overwrite protection (SEHOP)
REFERENCES	

## BUFFER OVERFLOW

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.5	
CVSSv3 CRITERIAS	Attack Vector : Attack Complexity : Required Privileges : User Interaction :	Local Low None Required	Scope : Confidentiality : Integrity : Availability :	Unchanged None None High
AFFECTED SCOPE				
DESCRIPTION	The Denial of Service (DoS) attack is focused on making 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.			
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				
<div></div>				
REMEDIATION	1. Input Sanitization 2. Addressing Buffer Overflow			
REFERENCES				