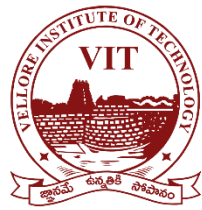


# VULNERABILITY REPORT



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

---

**MODIFICATIONS HISTORY**

Version	Date	Author	Description
1.0	05/17/2021	Chaitanya Ganesuni	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

## VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

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

## TECHNICAL DETAILS

### SHELL CODE INJECTION

CVSS SEVERITY	High	CVSSv3 SCORE	8.2
<b>CVSSv3 CRITERIAS</b>	Attack Vector : <b>Network</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>	Summary: Stored XSS can be submitted on reports, and anyone who will check the report the XSS will trigger. Description: Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.		
<b>OBSERVATION</b>	Steps To Reproduce: I wanted test on this site <a href="https://app.mopub.com/reports/custom/">https://app.mopub.com/reports/custom/</a> Now Click New network report. enter payload: "><img src=x onerror=alert(document.domain)>" in the Click Run and save then XSS will trigger. Demonstration of the vulnerability: PoC: xssed.webm (F412243) Tested on Firefox and chrome.		
<b>TEST DETAILS</b>			
<b>REMEDIATION</b>	The attacker can steal data from whoever checks the report.		
<b>REFERENCES</b>			

## BUFFER OVERFLOW

CVSS SEVERITY	High		CVSSv3 SCORE	7.6
CVSSv3 CRITERIAS	Attack Vector : <b>Local</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>
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

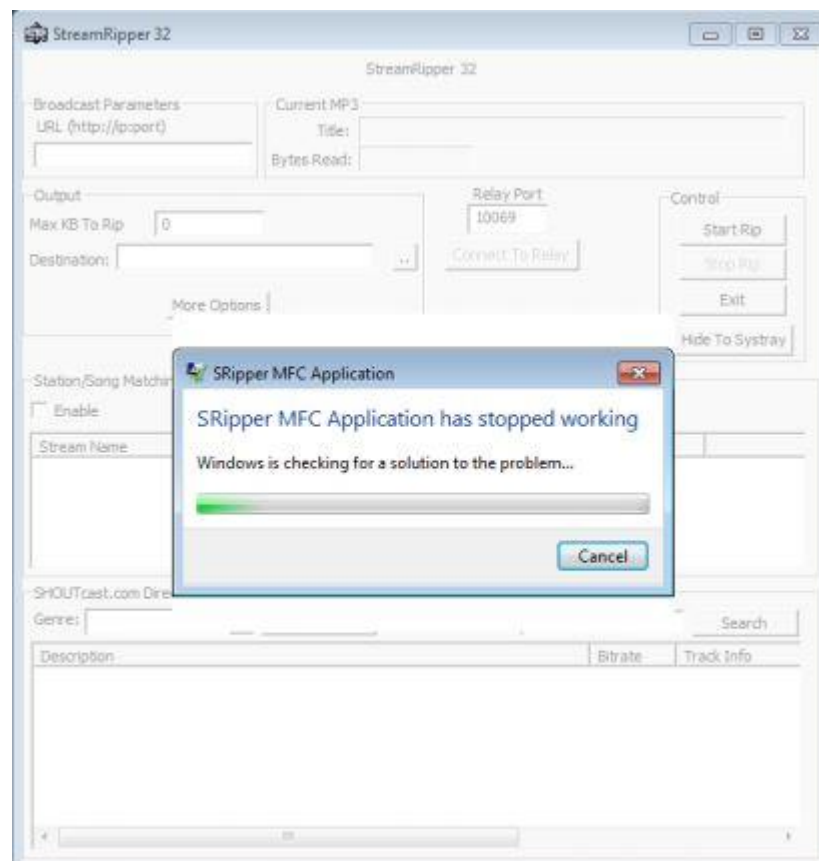
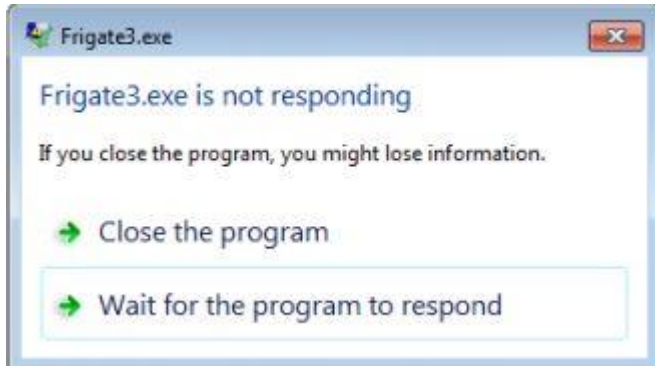




Image 1 – doc.JPG	
<b>REMEDIATION</b>	<ol style="list-style-type: none"><li>1. Address space randomization (ASLR)</li><li>2. Data execution prevention (DEP)</li><li>3. Structured exception handler overwrite protection (SEHOP)</li></ol>
<b>REFERENCES</b>	

## DENIAL OF SERVICE

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.5
<b>CVSSv3 CRITERIAS</b>	Attack Vector : <b>Local</b> Attack Complexity : <b>Low</b> Required Privileges : <b>None</b> User Interaction : <b>Required</b> Scope : <b>Unchanged</b> Confidentiality : <b>None</b> Integrity : <b>None</b> Availability : <b>High</b>		
<b>AFFECTED SCOPE</b>			
<b>DESCRIPTION</b>	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		
<b>OBSERVATION</b>	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		
<b>TEST DETAILS</b>	 <p>Image 2 – buff.JPG</p>		
<b>REMEDIATION</b>	1. Input Sanitization 2. Addressing Buffer Overflow		
<b>REFERENCES</b>			

