N.Shanmukh - 18BCE7292

Vulnerability Report

Thursday, May 27, 2021

VIT-AP
UNIVERSITY

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/27/2021	Narra Shanmukh	Initial Version

TABLE OF CONTENTS

General Information

Scope

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

- Software Security

Organisation

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

Executive Summary

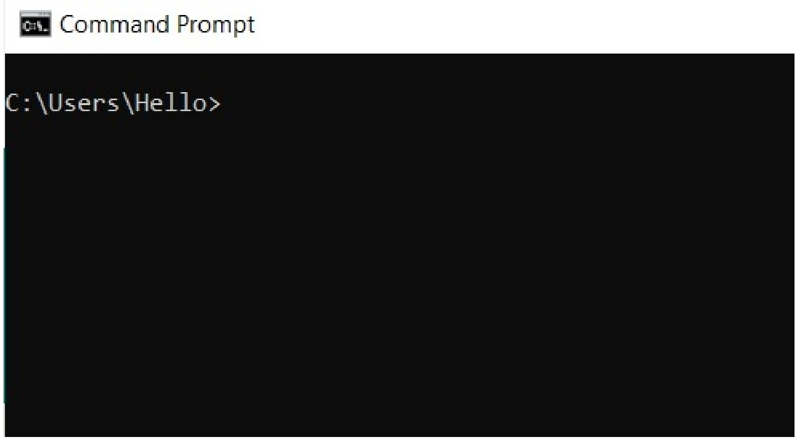
VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

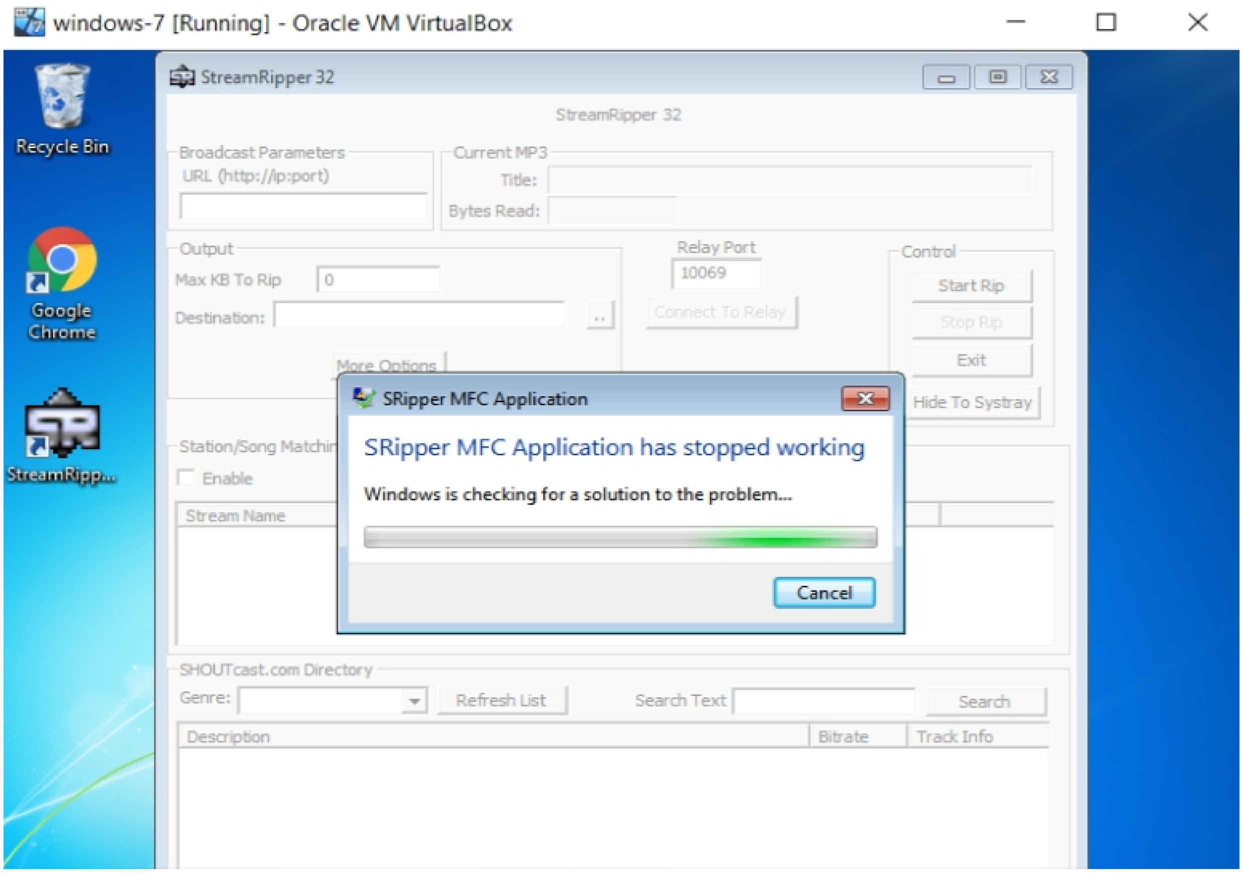
Risk	ID	Vulnerability	Affected Scope
High	IDX-003	Shell Code Injection	
High	IDX-001	Buffer Overflow	
Medium	VULN-002	Denial of Service	

Technical Details

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	Shell Code injection is the malicious injection or introduction of code into an application. The code introduced or injected is capable of compromising database integrity and/or compromising privacy properties, security and even data correctness. It can also steal data and/or bypass access and authentication control. Code injection attacks can plague applications that depend on user input for execution.			
Observation	I have identified that this Vulnerability can execute different malicious code and also triggers different applications including Command Prompt.			
Test details	 Command Prompt `C:\Users\Hello>`			
Remediation	1.Implementing ASLR, DEP, SEH 2. Addressing Buffer Overflow Vulnerability			
References				

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 happens when a program either tries to place data in a memory area past the buffer, or attempts to put more data in a buffer than it can hold. Writing data beyond an allocated memory block's bounds can crash the program, corrupt data, or allow an attacker to execute malicious code.			
Observation	I have observed that Buffer Overflow can crash an application and without user knowledge allows command Injection Attacks.			
Test Details 				

windows-7 [Running] - Oracle VM VirtualBox

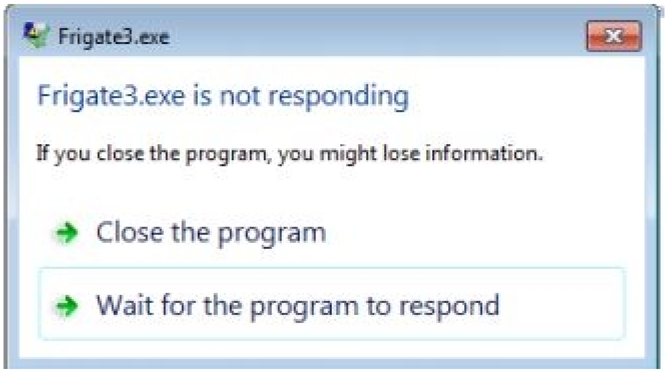
SRipper MFC Application

SRipper MFC Application has stopped working

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

REMEDIATION	1. Data execution prevention (DEP) 2. Structured exception handler overwrite protection (SEHOP) 3. Address Space Randomization (ASLR)
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	Denial-Of-Service (DoS) is an attack targeted at depriving legitimate users from online services. It is done by flooding the network or server with useless and invalid authentication requests which eventually brings the whole network down, resulting in no connectivity. As a result of this, users are prevented from using a service. A DoS attack is initiated by sending needless and superfluous messages to the server/network for authentication of requests having invalid return addresses.			
Observation	I have observed that the software crashes immediately as a result of having Large String input due to Buffer Overflow Vulnerability. This could impact the availability of the software			
Test Details	 Frigate3.exe is not responding If you close the program, you might lose information. 			
Remediation	1. Addressing Buffer Overflow 2. Input Sanitization			
References				