Buffer Overflow and Shell Code Injection in StreamRipper32 and Frigate

VULNERABILITY REPORT

FRIDAY, JUNE 11, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/11/2021	Nishit Verma	Initial Version

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE

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

- StreamRipper32
- Frigate

ORGANISATION

The testing activities were performed between 04/05/2021 and 04/21/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-002	Shell Code Injection	Frigate
Medium	VULN-001	Buffer Overflow	StreamRipper 32 and Frigate

TECHNICAL DETAILS

SHELL CODE INJECTION

CVSS SEVERITY	High		CVSSV3 SCORE	8.0
CVSSV3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE	Frigate			
DESCRIPTION	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 malicious codes. The hacker can easily deploy or execute any kind of code from a vulnerable field thus leading to many major issues or cyber attacks such as data loss, privilege escalation and ransomware attacks.			
OBSERVATION	This Vulnerability allows the hackers to exploit an application through a vulnerable user interaction field thus leading to many harmful unwanted activities such as data loss or leak, ransomware attacks, privilege escalation and even system take over.			

TEST DETAILS

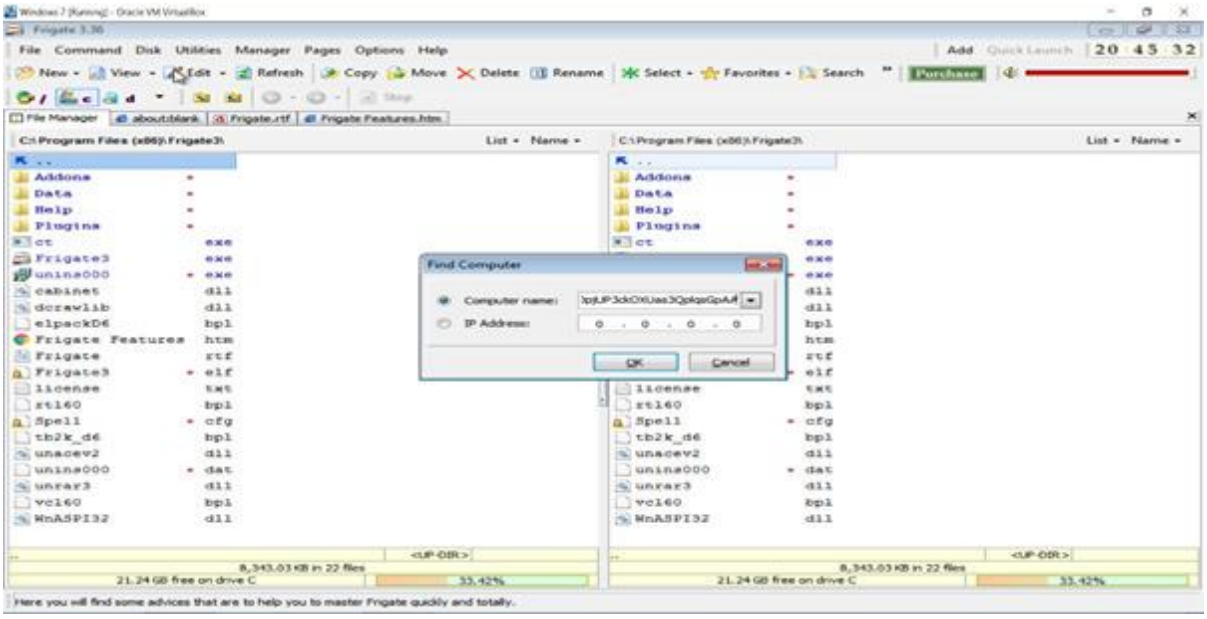

Image 1 – frigate.png

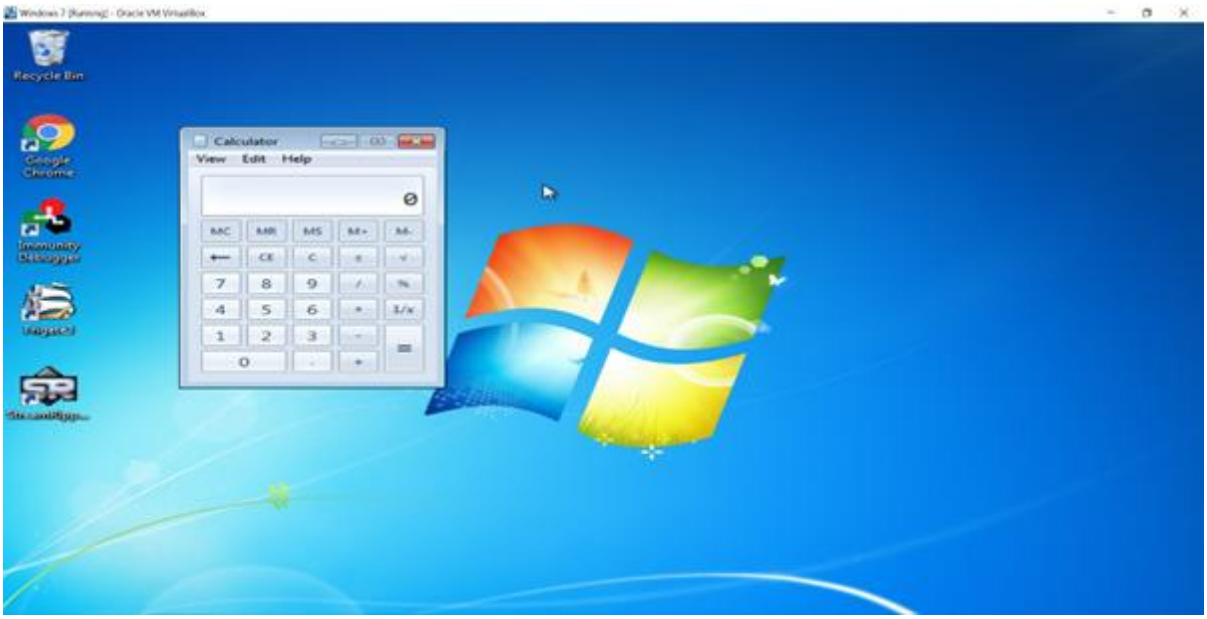

Image 2 – Shell Code Injection 1.png

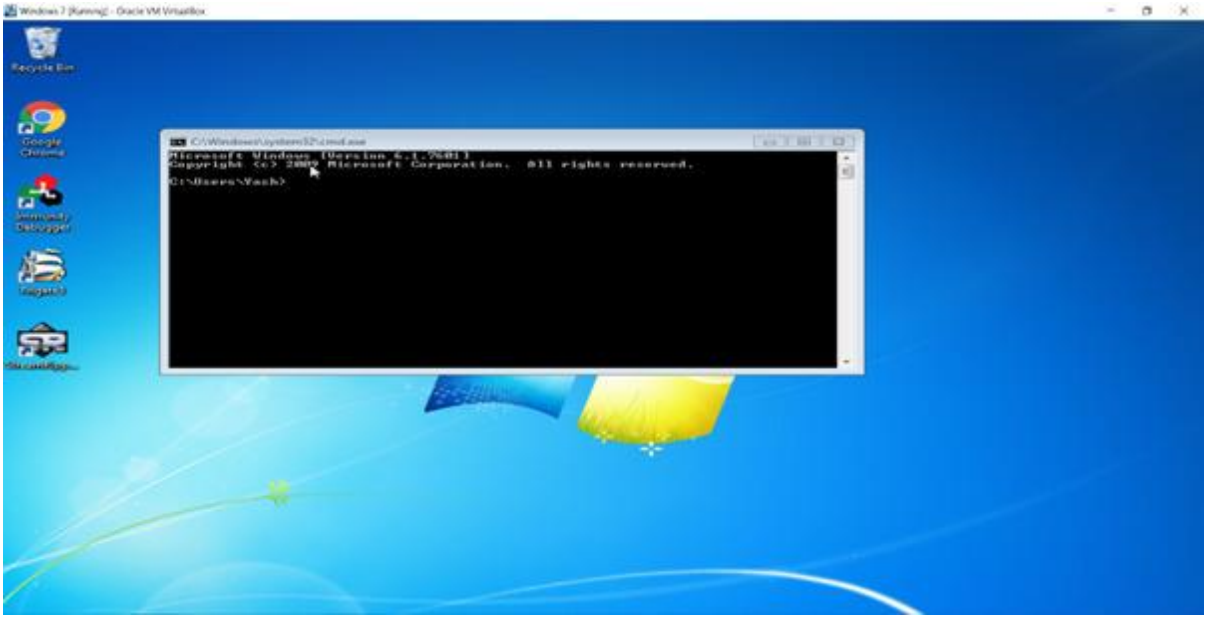

Image 3 – Shell Code Injection 2.png

REMEDIATION	The below steps could help in the prevention of this vulnerability 1. Input Sanitization 2. Addressing Memory vulnerabilities such as Buffer Overflow 3. Implementing DEP, ASLR and SEH
REFERENCES	

BUFFER OVERFLOW

CVSS SEVERITY	Medium		CVSSV3 SCORE	6.6
CVSSV3 CRITERIAS	Attack Vector :	**Local**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**Low**
	Required Privileges :	**None**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE	StreamRipper 32 and Frigate			
DESCRIPTION	Buffer Overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations thus making the application vulnerable to data leaks, unauthorized access and also results in crashes.			
OBSERVATION	Buffer Overflow attack crashes the application and even sometimes leads to probable injection of malicious code through the exploitable input area or region.			

TEST DETAILS

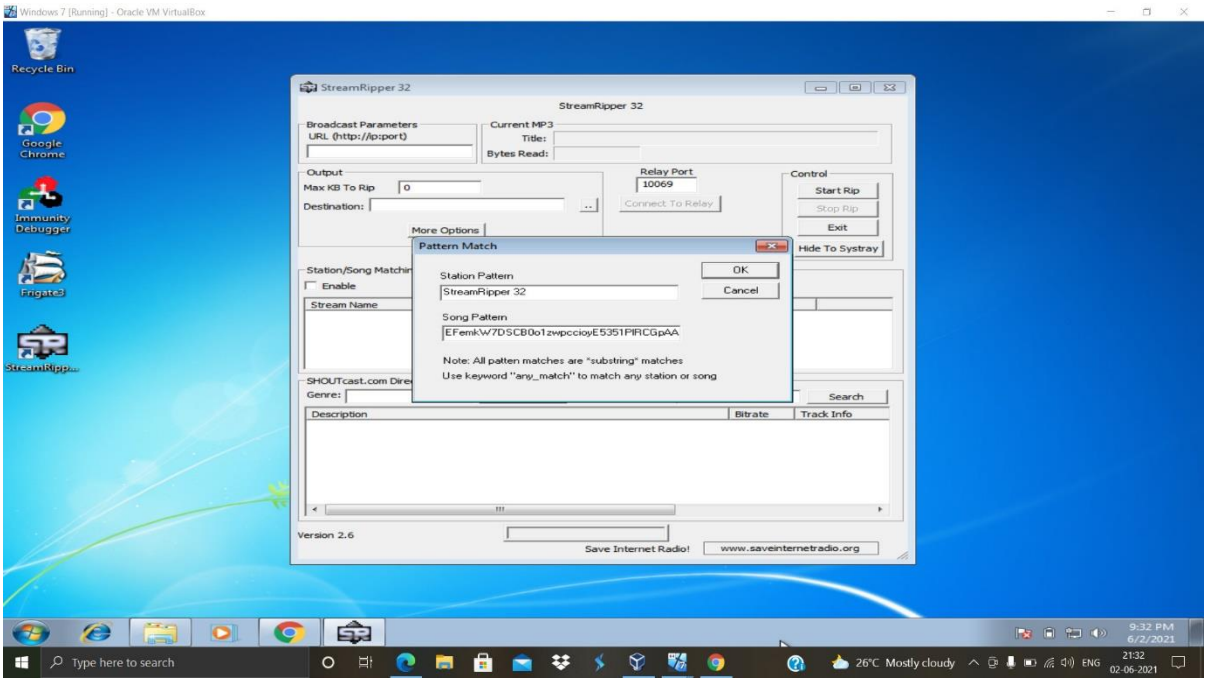

Image 4 – StreamRipper32.png

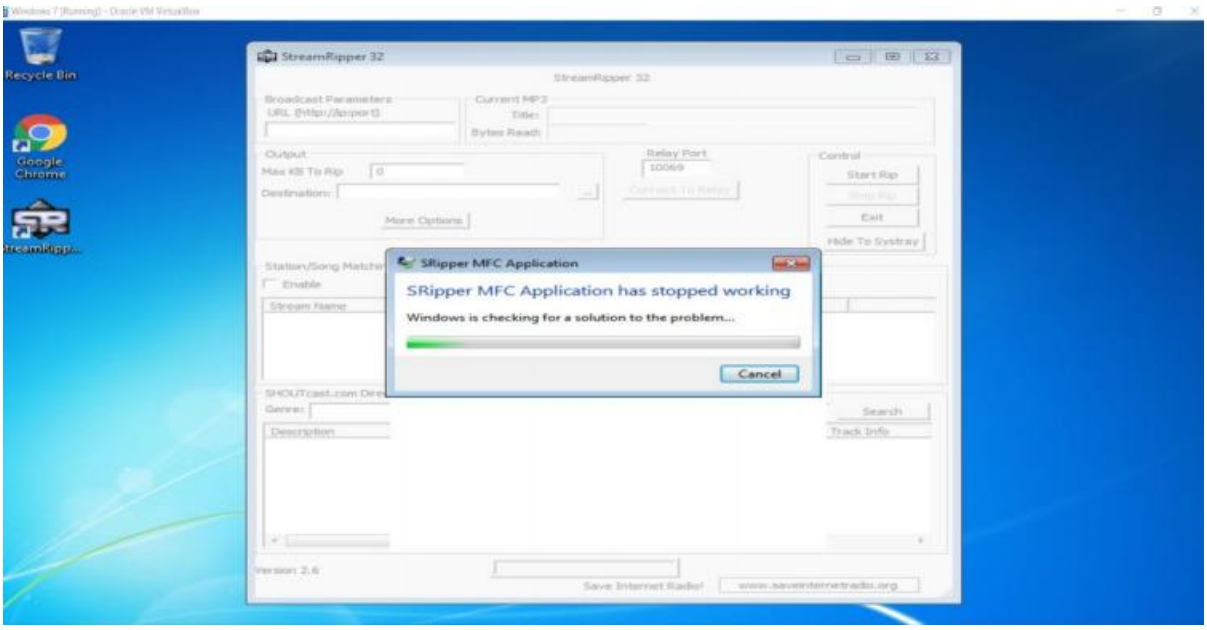

Image 5 – Buffer Overflow.PNG

REMEDIATION	The following should be implemented to avoid buffer overflow attacks 1. Data Execution Prevention (DEP) 2. Address Space Randomization (ASLR) 3. Structured Exception Handler and Overwrite Protection (SEHOP)
REFERENCES	