Buffer Overflow and Shell Code Injection in StreamRipper32 and Frigate

VULNERABILITY REPORT

SUNDAY, JUNE 13, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/13/2021	Nishank 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 04/10/2021 and 04/25/2021.

EXECUTIVE SUMMARY

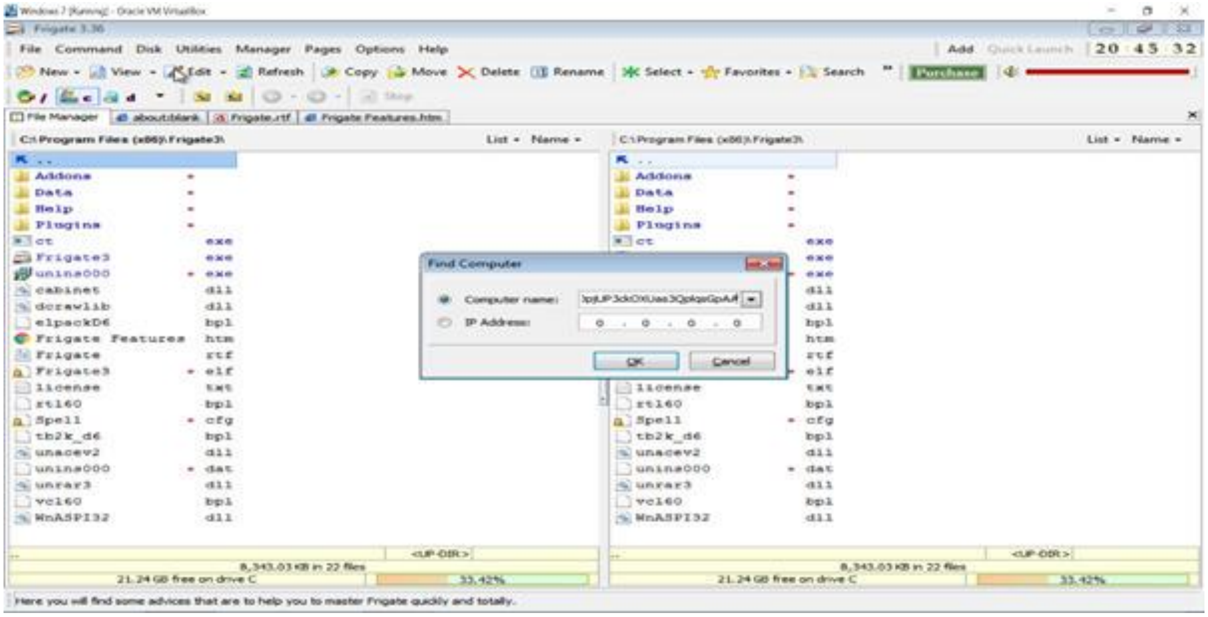
VULNERABILITIES SUMMARY

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	The Vulnerability discovered can effect the system extensively and can lead to different types of attack on computer or system by hackers.			
Test Details	 Find Computer ● Computer name:)pjUP3ckOXUas3QpAqsGpA# ○ IP Address: 0 . 0 . 0 . 0 Image 1 – frigate.png			

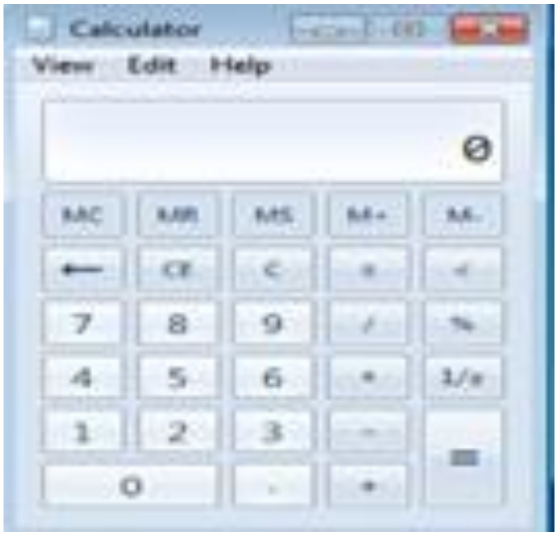
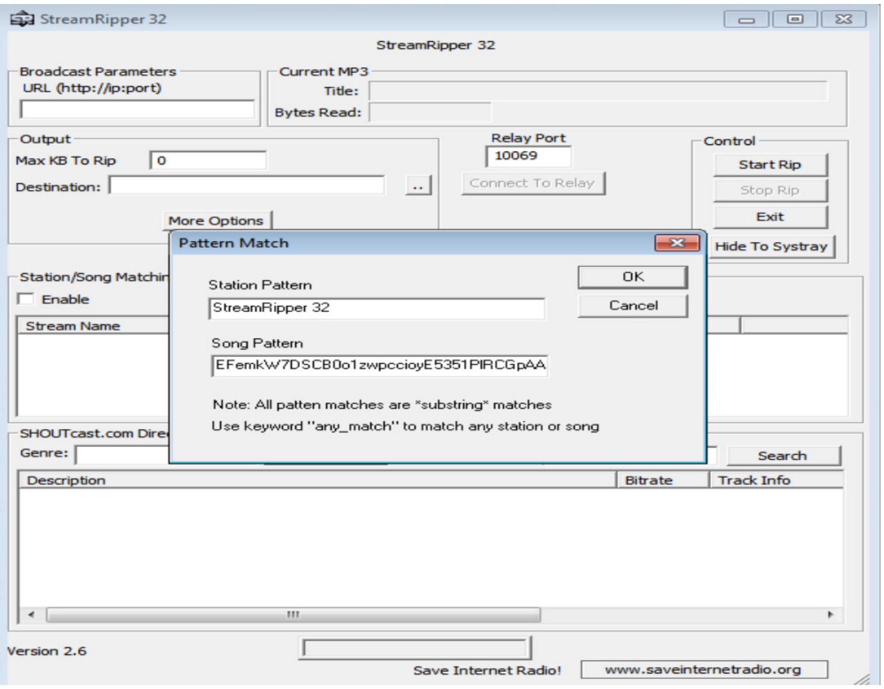
<table>
<tr><td colspan="2">

Image 2 – Shell Code Injection 1.png</td></tr>
<tr><td><b>REMEDIATION</b></td><td>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</td></tr>
<tr><td><b>REFERENCES</b></td><td></td></tr>
</table>

Buffer Overflow

CVSS Severity	**Medium**		**CVSSv3 Score**	**6.6**
CVSSv3 **Criterias**	Attack Vector : Attack Complexity : Required Privileges : User Interaction :	**Local** **Low** **None** **Required**	Scope : Confidentiality : Integrity : Availability :	**Unchanged** **Low** **Low** **High**
Affected Scope	StreamRipper 32 and Frigate			
Description	A buffer overflow condition 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	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



Max KB To Rip: 0

Relay Port: 10069

Station Pattern: StreamRipper 32

Song Pattern: EFemkW7DSCB0o1zwpccioyE5351PIRCGpAA

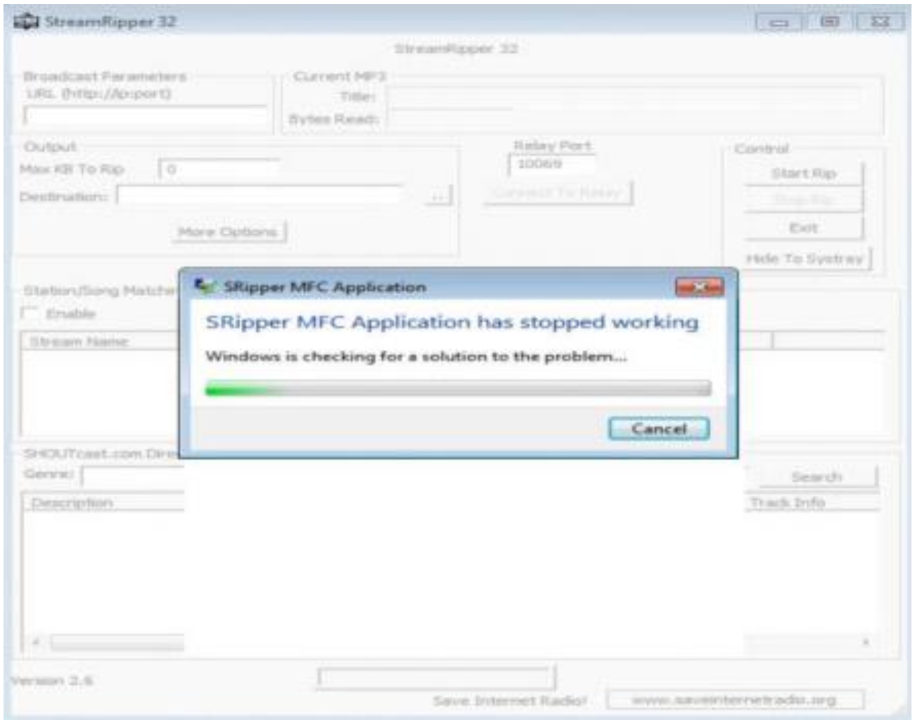
Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Version 2.6

www.saveinternetradio.org

Image 3 – StreamRipper32.png

<table>
<tr><td colspan="2">

StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
...
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matcher
Enable
Stream Name
SHOUTcast.com Directory
Genre:
Search
Description
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org
SRipper MFC Application
Cancel

SRipper MFC Application has stopped working
Windows is checking for a solution to the problem...
Image 4 – Buffer Overflow.PNG</td></tr>
<tr><td><strong>REMEDIATION</strong></td><td>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)</td></tr>
<tr><td><strong>REFERENCES</strong></td><td></td></tr>
</table>