CONFIDENTIAL

Stream Ripper 32 Frigate

VULNERABILITY REPORT

Friday,JUNE 11, 2021

VIT-AP UNIVERSITY

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/11/2021	Rishav Dhiman	Initial Version

TABLE OF CONTENTS

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:

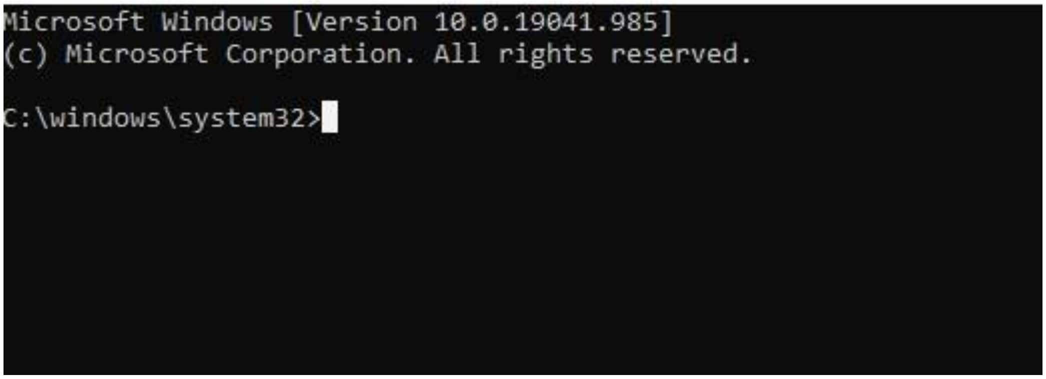
Risk	ID	Vulnerability	Affected Scope
High	IDX-003	Shell Code Injection	
High	IDX-001	Buffer Overflow	
Medium	VULN-002	Denial of service	

Technical Details{#findings}

SHELL CODE INJECTION

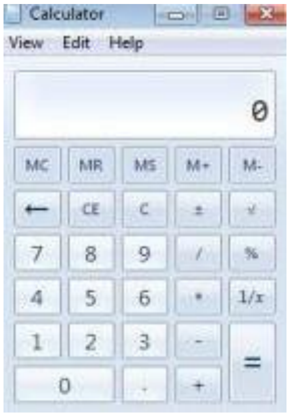
CVSS Severity	High		**CVSSv3 Score**	**8.2**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	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.			
Observation	We have identified that this Vulnerability can execute different malicious code and can even trigger different applications including Command Prompt.			

Test details



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

C:\windows\system32>
```

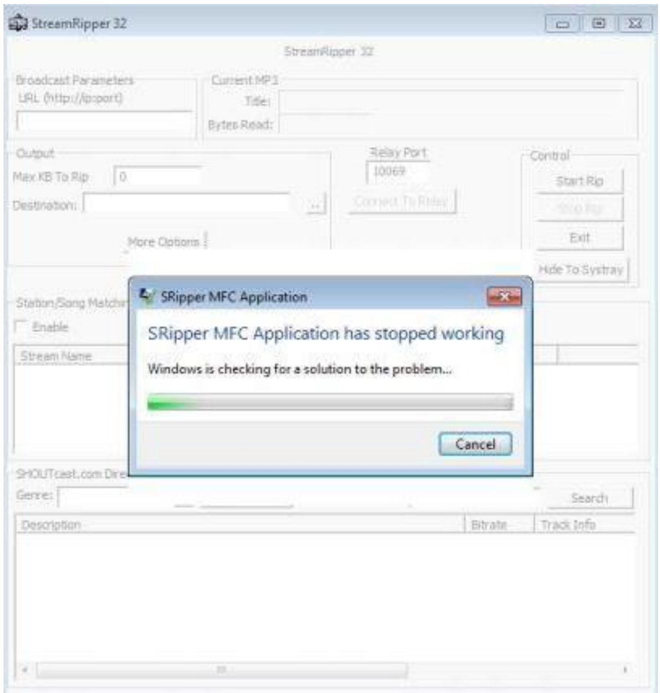


Remediation	1. Addressing Buffer Overflow Vulnerability 2. Input Sanitization 3. Implementing ASLR, DEP, SEH
References	

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, 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

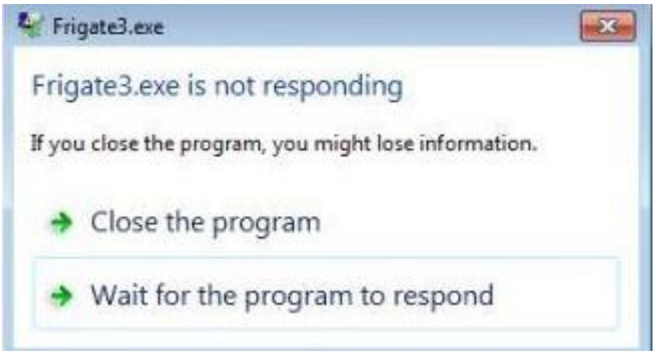


SRipper MFC Application has stopped working

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

Remediation	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 :	**Local**	Scope :	**Unhanged**
	Attack Complexity :	**Low**	Confidentiality :	**None**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**Required**	Availability :	**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  Frigate3.exe Frigate3.exe is not responding If you close the program, you might lose information. Close the program Wait for the program to respond				
Remediation	1. Input Sanitization 2. Addressing Buffer Overflow			
References				