

Stream Ripper 32 Frigate

VULNERABILITY REPORT

Friday, JUNE 11, 2021



VIT-AP UNIVERSITY



CONFIDENTIAL

MODIFICATIONS HISTORY

Version	Date	Author Description
1.0	06/11/2021	Devashish Kankanwar Initial Version

1. General Information	4
1.1 Scope	4
1.2 Organisation	4
2. Executive Summary	5
3. Technical Details	6
3.1 title	6
4. Vulnerabilities summary	8

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.



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	

6 / 11



CONFIDENTIAL TECHNICAL DETAILS{#FINDINGS}

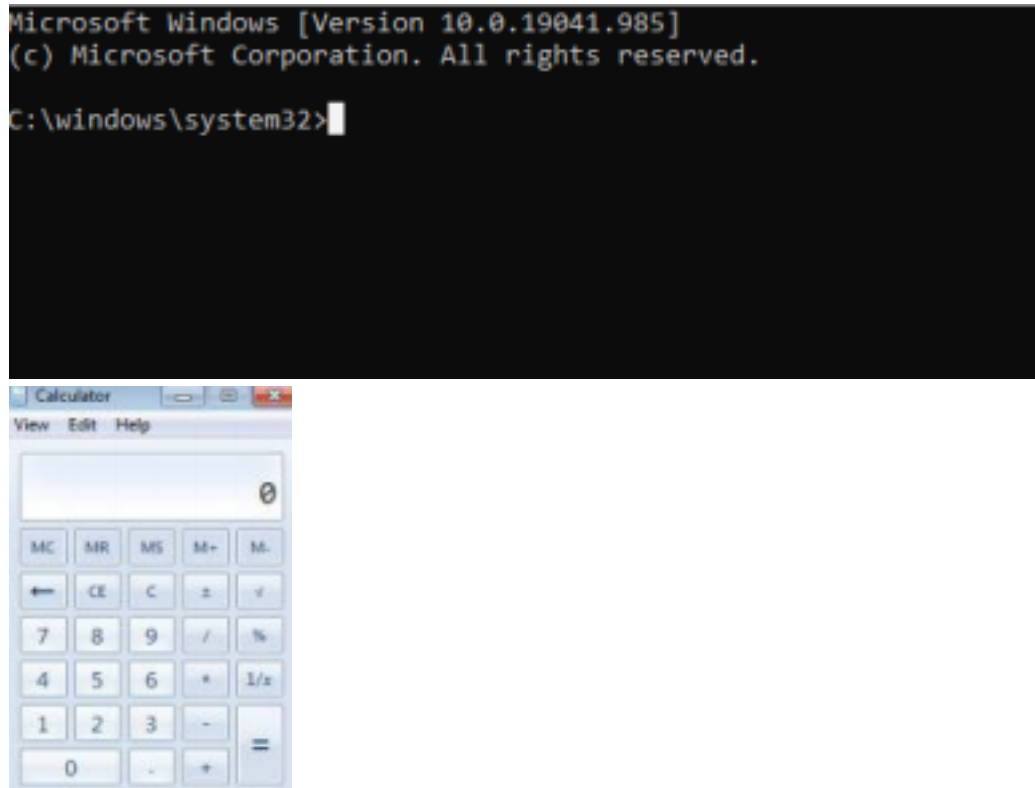
SHELL CODE INJECTION

CVSS SEVERITY	High CVSSv3 SCORE
CVSSv3 CRITERIAS	<p>Attack Vector : Network Scope : Changed Attack Complexity : High</p> <p>Confidentiality : High</p> <p>Required Privileges : None Integrity : Low</p> <p>User Interaction : Required Availability : High</p>
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. The 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.

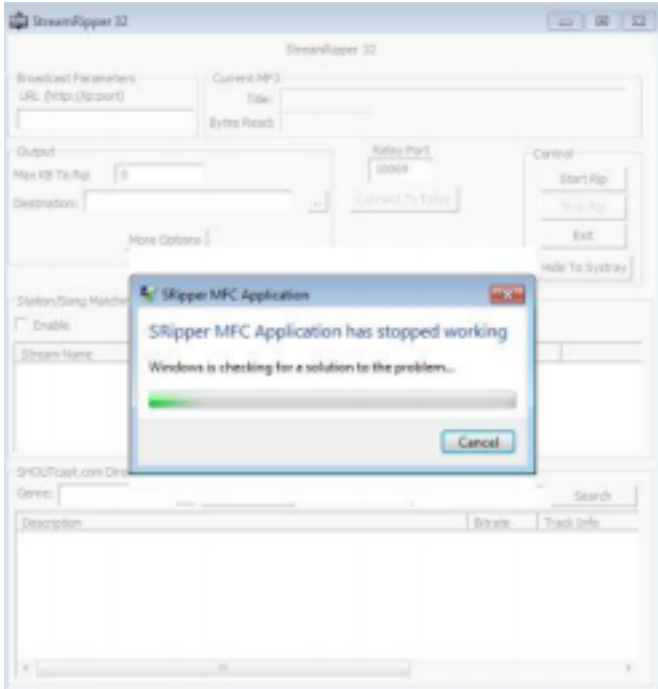
TEST DETAILS



7 / 11

REMEDIATION	1. Addressing Buffer Overflow Vulnerability 2. Input Sanitization 3. Implementing ASLR, DEP, SEH
REFERENCES	

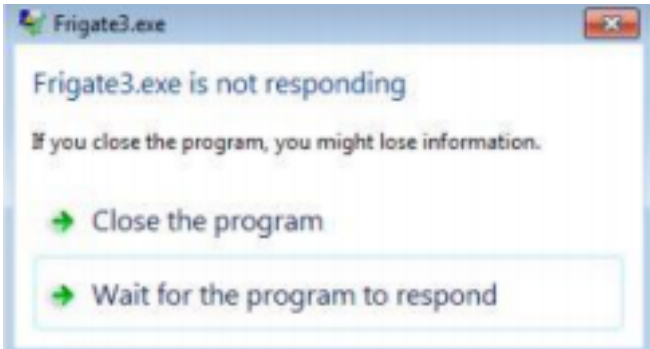
8 / 11

CVSS SEVERITY	High CVSSv3 SCORE
CVSSv3 CRITERIAS	<p>Attack Vector : Local Scope : Changed Attack Complexity : High Confidentiality : High</p> <p>Required Privileges : None Integrity : Low</p> <p>User Interaction : Required Availability : High</p>
AFFECTED SCOPE	<p>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.</p> <p>OBSERVATION We have observed that this buffer overflow can potentially crash an application and unknowingly allows command injection attacks.</p> <p>TEST DETAILS</p> 
REMEDIATION	<ol style="list-style-type: none"> 1. Address space randomization (ASLR) 2. Data execution prevention (DEP)

	3. Structured exception handler overwrite protection (SEHOP)
REFERENCES	

10 / 11

BUFFER OVERFLOW

CVSS SEVERITY	Medium CVSSv3 SCORE
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.
<p>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</p> <p>TEST DETAILS</p> 	
REMEDIATION	1. Input Sanitization 2. Addressing Buffer Overflow
REFERENCES	

