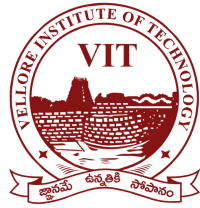


N.V.SOWMITH - 18BCE7338

VULNERABILITY REPORT

SUNDAY, MAY 23, 2021



VIT-AP

UNIVERSITY

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/23/2021	Narra Venkata Sowmith	Initial Version

TABLE OF CONTENTS

1.	General Information.....	4
1.1	Scope.....	4
1.2	Organisation.....	4
2.	Executive Summary.....	5
3.	Technical Details.....	6
3.1	title.....	7
4.	Vulnerabilities summary.....	6

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

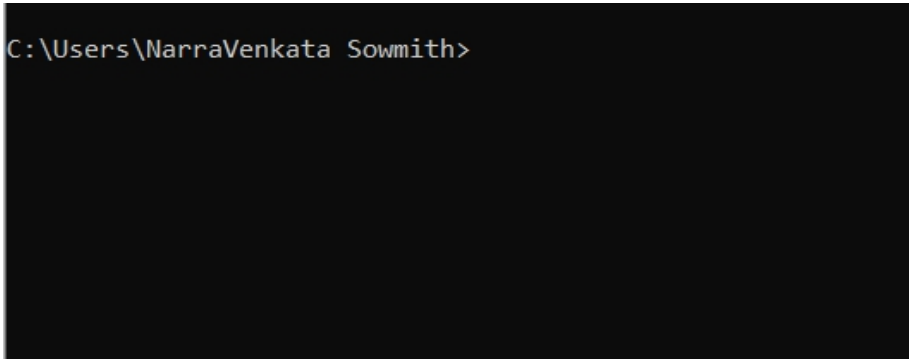
VULNERABILITIES SUMMARY

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

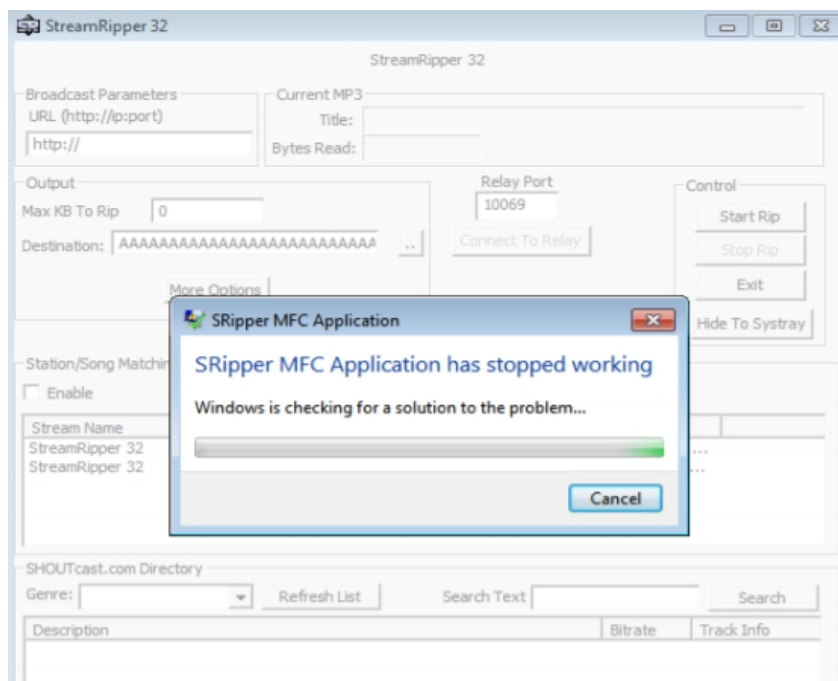
SHELL CODE INJECTION

CVSS SEVERITY	High	CVSSv3 SCORE	8.2
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : High Required Privileges : None User Interaction : Required Scope : Changed Confidentiality : High Integrity : Low Availability : High		
AFFECTED SCOPE			
DESCRIPTION	A shellcode refers to a small piece of code that is used for exploiting a vulnerability of a software. The name is a node to shellcode's ability to start a command shell through which the hacker gains the control of the compromised device. Shell code injection is a hacking technique where the hacker exploits vulnerable programs.		
OBSERVATION	I have identified that this Vulnerability can execute different malicious code and can even trigger different applications including Command Prompt.		
TEST DETAILS			
REMEDIATION	1. Implementing ASLR, DEP, SEH 2. Addressing Buffer Overflow Vulnerability 3. Implementing ASLR, DEP, SEH		
REFERENCES			

BUFFER OVERFLOW

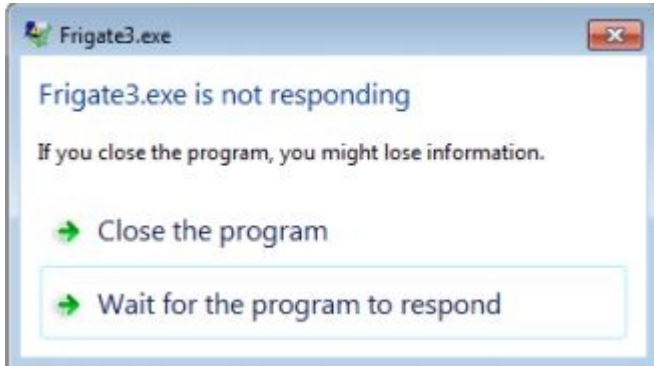
CVSS SEVERITY	High	CVSSV3 SCORE	7.6
CVSSV3 CRITERIAS	Attack Vector : Local Attack Complexity : High Required Privileges : None User Interaction : Required Scope : Changed Confidentiality : High Integrity : Low Availability : High		
AFFECTED SCOPE			
DESCRIPTION	A buffer overflow occurs when a program or process attempts to write more data to a fixed length block of memory, or buffer, than the buffer is allocated to hold. Since buffers are created to contain a defined amount of data, the extra data can overwrite data values in memory addresses adjacent to the destination buffer unless the program includes sufficient bounds checking to flag or discard data when too much is sent to a memory buffer. Exploiting a buffer overflow allows an attacker to control or crash the process or to modify its internal variables. Buffer overflow always ranks high in the Common Weakness Enumeration. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.		
OBSERVATION	I have observed that Buffer Overflow can crash an application and without user knowledge allows command Injection Attacks.		

TEST DETAILS



REMEDIATION	<ol style="list-style-type: none">1. Data execution prevention (DEP)2. Structured exception handler overwrite protection (SEHOP)3. Address Space Randomization
REFERENCES	

DENIAL OF SERVICE

CVSS SEVERITY	Medium	CVSSV3 SCORE	5.5
CVSSV3 CRITERIAS	Attack Vector : Local Attack Complexity : Low Required Privileges : None User Interaction : Required Scope : Unchanged Confidentiality : None Integrity : None Availability : High		
AFFECTED SCOPE			
DESCRIPTION	A Denial-of-Service attack (DOS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.		
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			
REMEDIATION	1. Input Sanitization 2. Addressing Buffer Overflow		
REFERENCES			