Lab-12

VULNERABILITY REPORT

MONDAY, MAY 17, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/17/2021	Amritesh Dasari	Initial Version

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE

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

ORGANISATION

The testing activities were performed between 05/17/2021 and 05/17/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

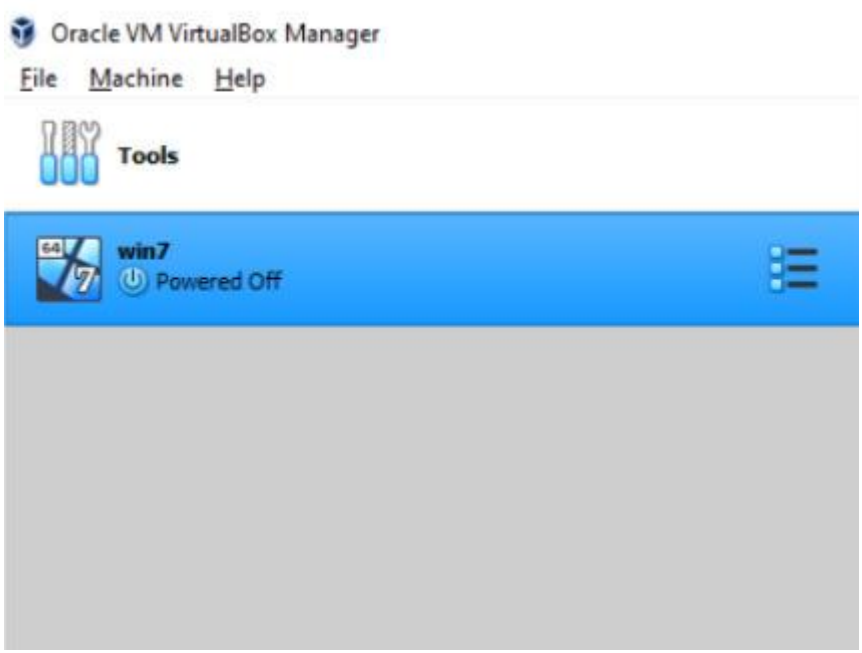
Risk	ID	Vulnerability	Affected Scope
Medium	VULN-004	Buffer Overflow StreamRipper32	
Medium	VULN-003	Buffer Overflow Frigate 2	
Medium	VULN-002	Buffer Overflow Frigate	

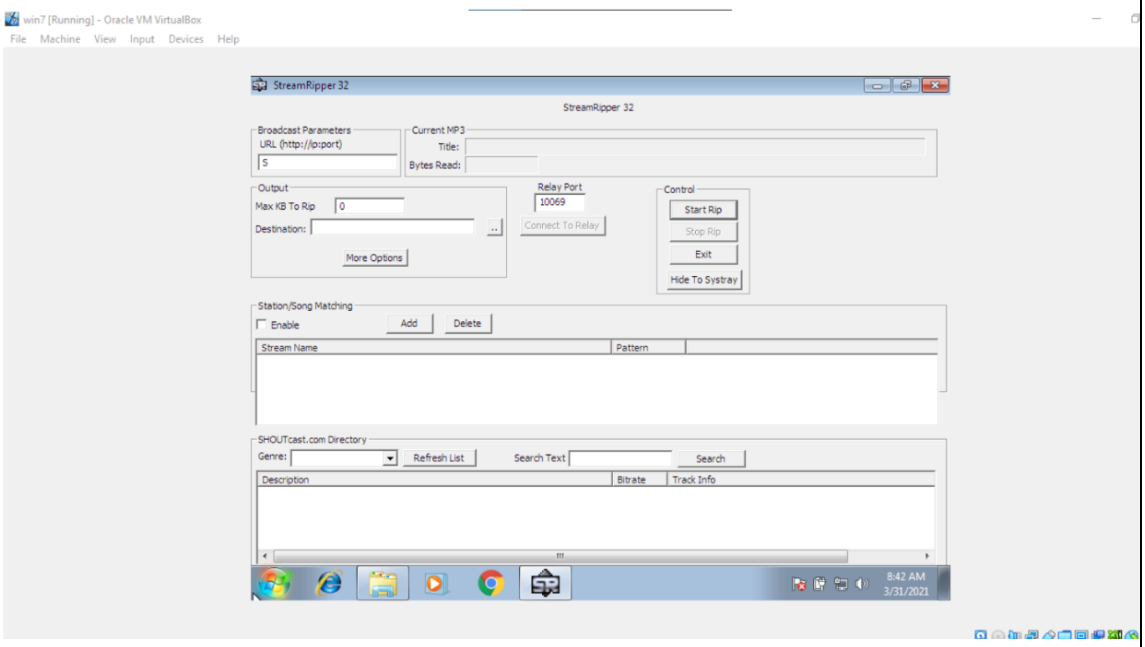
TECHNICAL DETAILS

BUFFER OVERFLOW STREAMRIPPER32

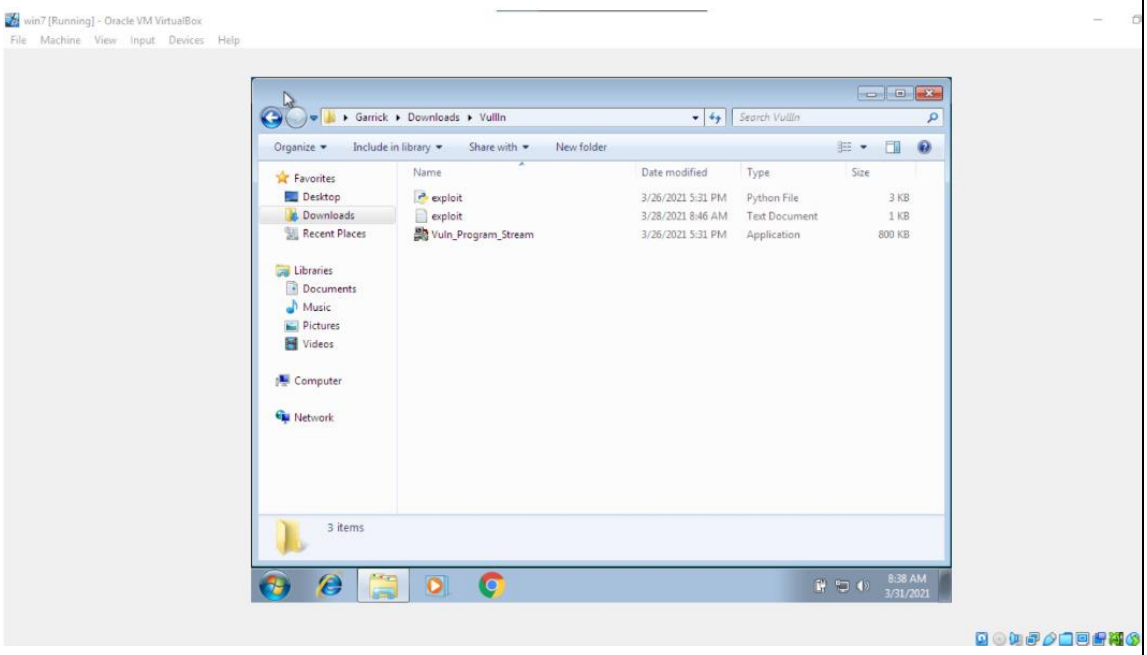
CVSS SEVERITY	**Medium**		**CVSSV3 SCORE**	**5.9**
CVSSV3 CRITERIAS	Attack Vector :	**Physical**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**None**
	Required Privileges :	**None**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
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	Install StreamRipper32 on Windows 7 VM

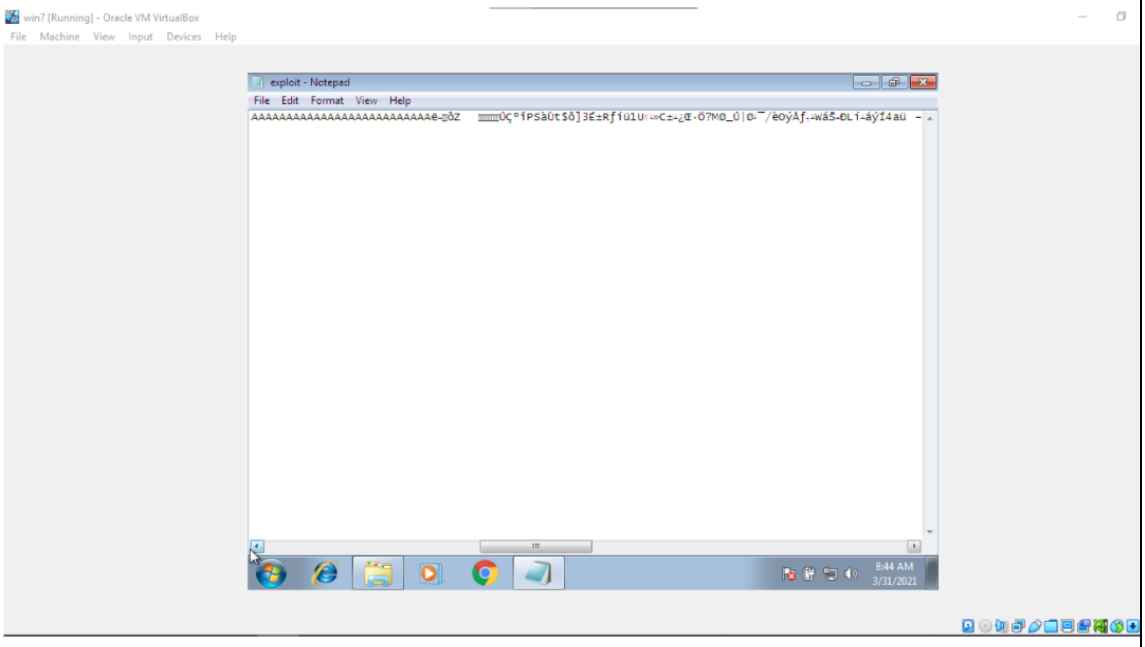




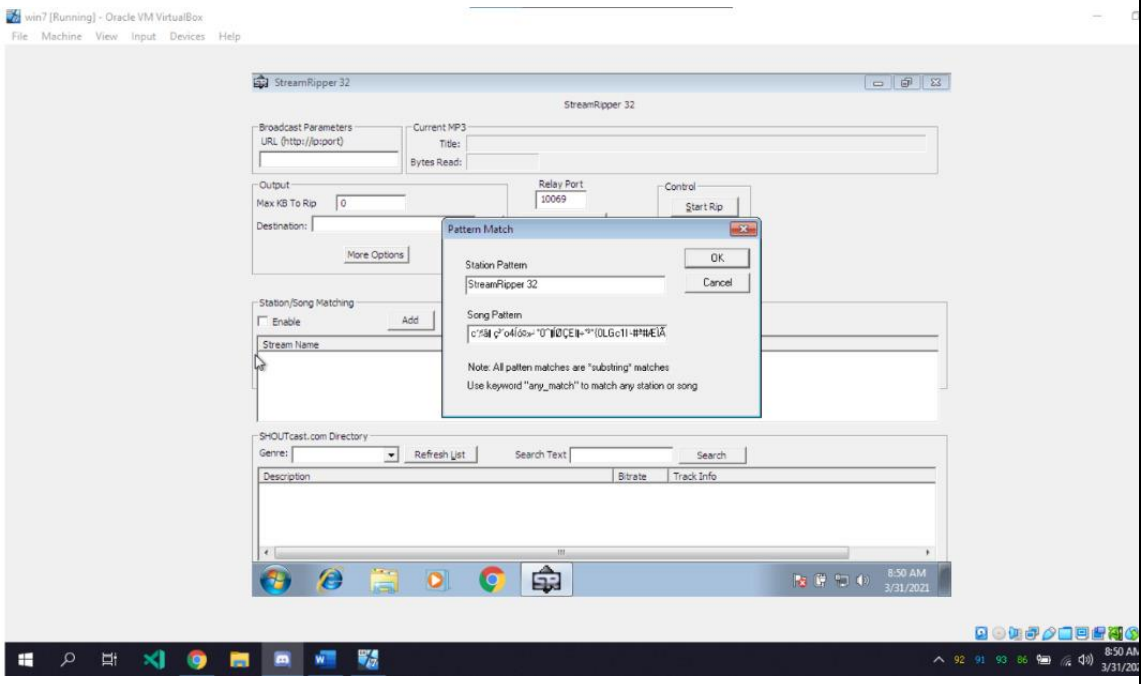
Extract the Zip file to get the application executable and a python file:



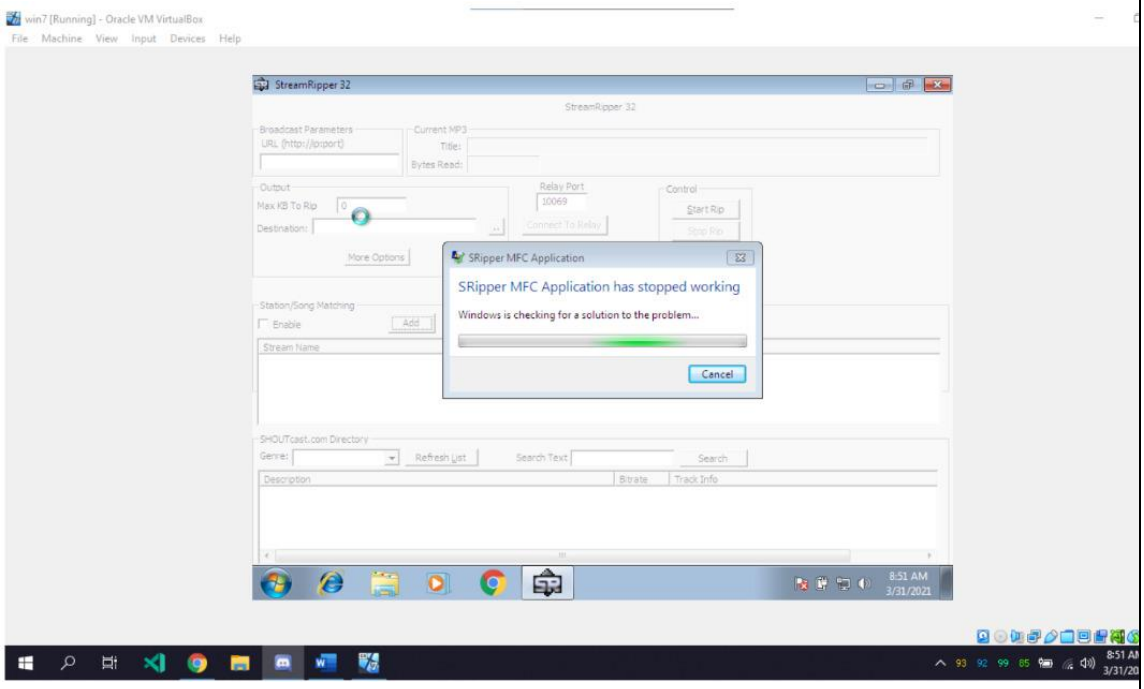
Because this is a fresh install of windows 7 and because official support for windows 7 ended a while ago, we had to install python 2.7.17 and Chrome to download the files and to execute the py file. After executing the python file, we get a new exploit.exe file which has the required payload for the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



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



And the Application crashes



TEST DETAILS

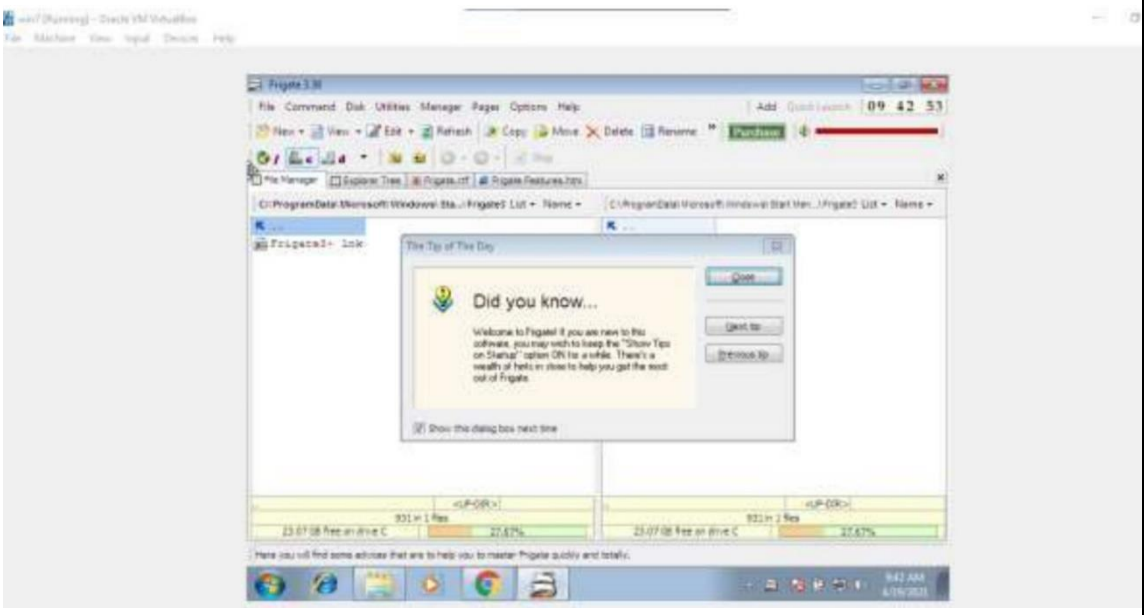
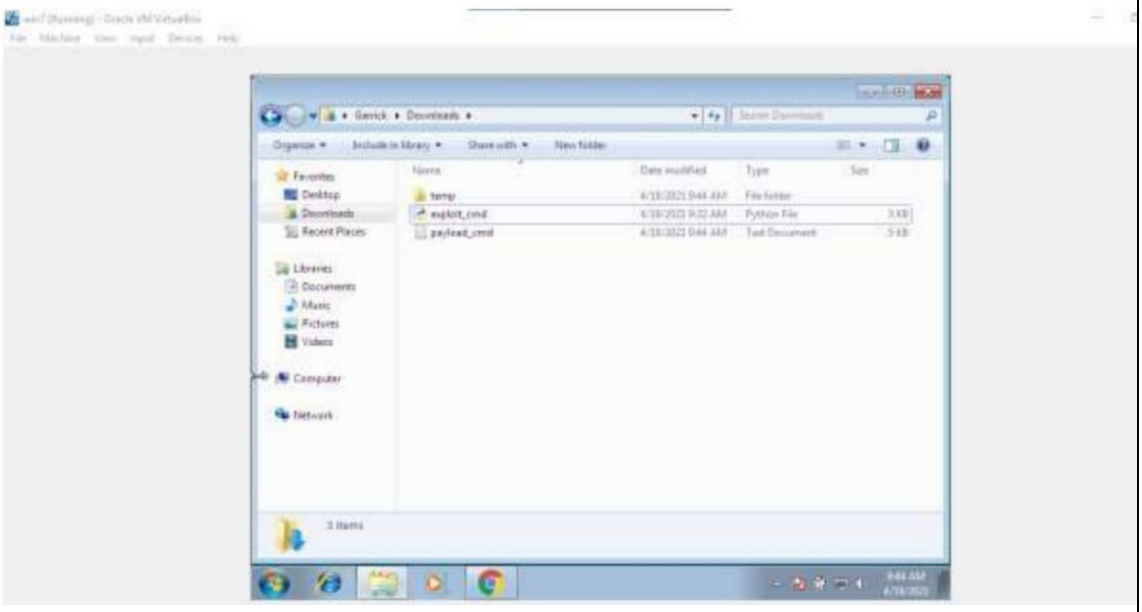
REMEDIATION	Why the Application crashes: So when the input in that text field exceeds 256 characters, Buffer Overflow happens and that causes the application to crash, because it is not being handled properly. This vulnerability can be easily fixed by limiting the number of characters that specific field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

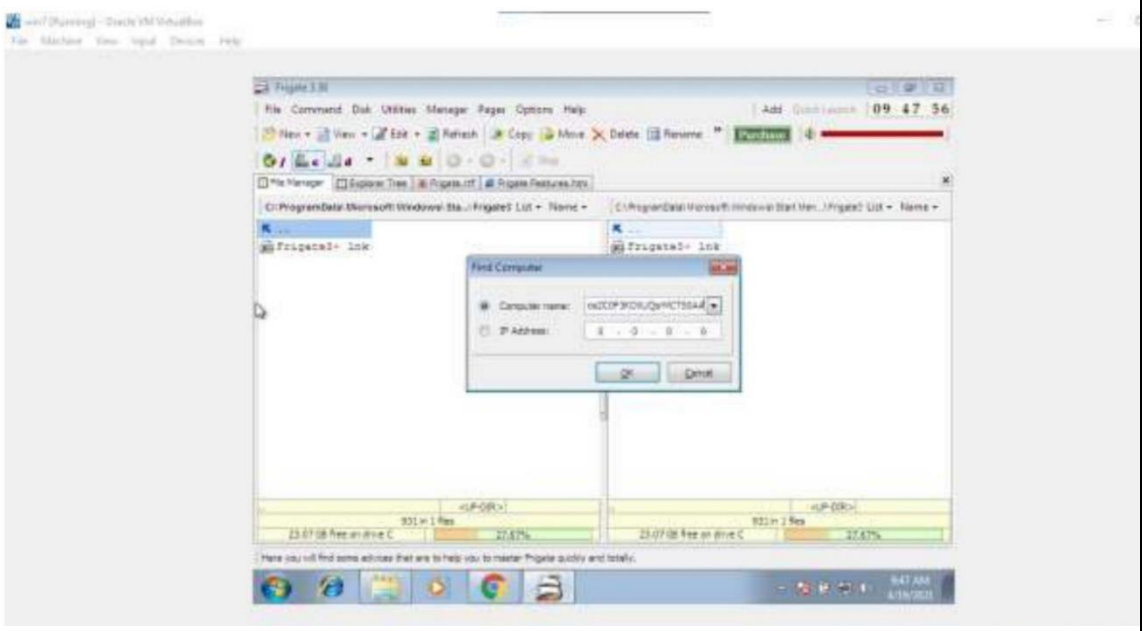
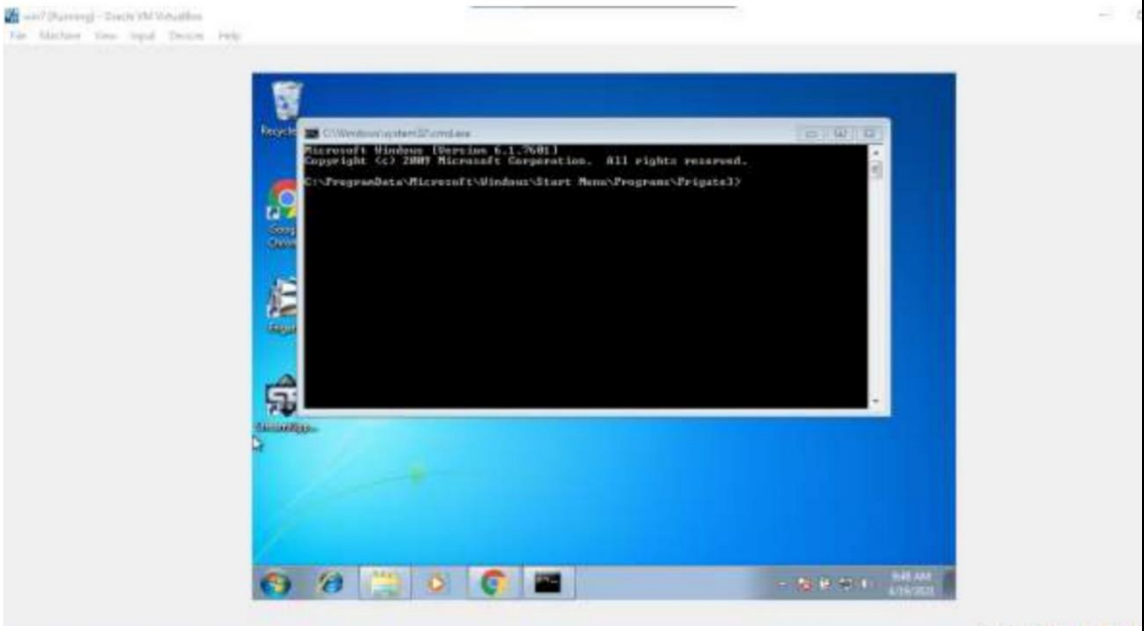
BUFFER OVERFLOW FRIGATE 2

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**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**None**
	Required Privileges :	**None**	Integrity :	**Low**
	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	Install Frigate3 on Windows 7 VM:  Execute the exploit2.py to generate the payload_cmd.txt file:  Copy the payload and open the frigate software, Go to disks and select find computer and paste the payload in it.

	  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 : Attack Complexity : Required Privileges : User Interaction :	Scope : Confidentiality : Integrity : Availability :	
AFFECTED SCOPE			
DESCRIPTION			
OBSERVATION	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		
TEST DETAILS			
REMEDIATION			
REFERENCES			