

GoodSecurity Penetration Test Report

[Robert L. Myers@GoodSecurity.com](mailto:Robert.L.Myers@GoodSecurity.com)

October 24, 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 exploiting 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

```
root@kali: # nmap -sS -sV -O -Pn 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-21 20:22 PDT
Nmap scan report for 192.168.0.20
Host is up (0.012s 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         Iccast 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=10/21%OT=25%CT=1%CU=41642%PV=Y%DS=1%DC=D%G=Y%M=00155D%
OS:TM=61722E7E%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=107%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%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=0%A=S+
OS:%F=A%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=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%O=0%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%O=0%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 23.36 seconds
root@kali: #
```

Hostname: **MSEEDGEWIN10**

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

Windows IP Configuration

Host Name . . . . . : MSEEDGEWIN10
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
```

Vulnerability Exploited: **Iccast Header Overwrite**

- Search for Iccast using msfconsole to display the Iccast Header Overwrite exploit

```
msf5 > search Iccast

Matching Modules
=====

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

msf5 >
```

- **Upon further Investigation** we also determined that there is a total of 9 publicly known vulnerability's on the Iccast streaming media server.
- The 9 vulnerabilities listed in the picture below can also be found at the following public website: <https://www.exploit-db.com/>
- This website is a popular public source of information documenting potential vulnerabilities. Simply search for Iccast and these 9 vulnerabilities will be displayed for any potential attacker to see. The vulnerability has been assigned the identifier CVE-2018-18820.

```
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 - AVLib 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
-----

Shellcodes: No Results
Papers: No Results
root@kali:~#
```

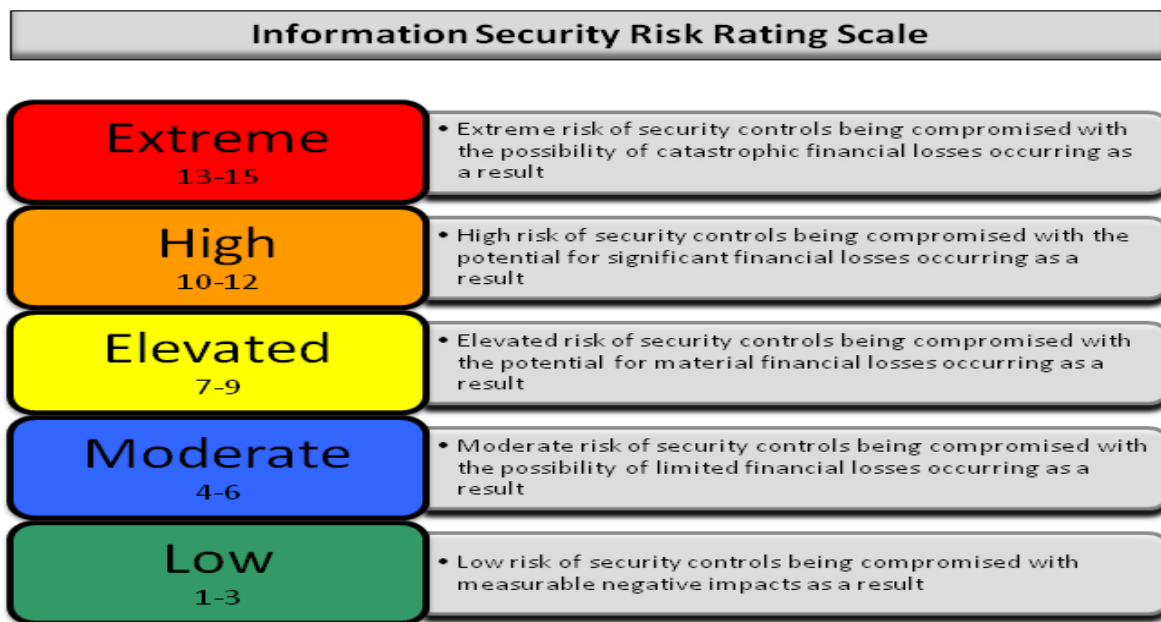
Vulnerability Explanation:

The Icecast Header Overwrite exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. This exploit will send 32 HTTP headers and cause a write one past the end of a pointer array. Basically, this can cause the system to crash or allow the attacker to establish remote access to the server or user.

In this specific example, GoodSecurity was able to establish a remote code access connection allowing the Penetration Team to see all files and directories inside the Icecast server, specifically GoodCorp's CEO, Hans Gruber and the two files: user.secretfile.txt and Drinks.recipe.txt

Severity:

GoodSecurity's expert opinion this vulnerability would be **EXTREME**



Proof of Concept:

3.0 Recommendations

What recommendations would you give to GoodCorp?