GoodSecurity Penetration Test Report

[Arctos.Morei@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

03/03/2022

# 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans’ computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on Hans’ computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Findings

Machine IP:

192.168.0.20

Hostname:

DVW10 - MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite

Vulnerability Explanation:

This vulnerability allows us to gain access to the victim device using Icecast as a backdoor into the application.

Severity:

This exploit’s CVSS is 7.5, which is high due to the fact that code execution can be performed remotely. As an attacker, I was able to access two files that were deemed secret, enumerated logged on users, and was able to get a hash dump of their passwords, which can then be put through John the Ripper to retrieve the actual passwords being used. As such, we now know the Admin’s account password is “Passw0rd!”.

# Proof of Concept

Since we are only allowed to scan the CEO’s device IP, we logged into DVWA10 and ran ifconfig to determine the victim’s IP. It’s 192.168.0.20.

Text

Description automatically generated

Text

Description automatically generated

From there, we ran an nmap to scan the victim’s IP for open ports.

Graphical user interface, text, application

Description automatically generated

For the purposes of exploiting Icecast, we can see that port 8000 is open, leaving it susceptible to exploitation. It’s time to open up Metasploit.

Text

Description automatically generated

From within MetaSploit, we are able to search for exploits. Using the command “search icecast”, we see that the exploit “icecast\_header” is available and that its option # is 0.

Graphical user interface, text, application

Description automatically generated

With the command “use 0”, we can begin editing the exploit to attack our target. To do this, we must edit the RHOSTS file to reflect our target IP and then run the exploit.

Text

Description automatically generated

Now that the RHOSTS is set and the exploit is running, we can easily use meterpreter to gain access to all sorts of things. For example, from here I could use getsystem and shell to gain access through a new channel.  
Text

Description automatically generated

Once I had access, I could run a systeminfo or even a sysinfo in meterpreter to find out that the Computer’s name is MSEDGEWIN10, among other info.

Text

Description automatically generated

Or I could run ps to see what services are currently running, allowing me to find a more stable process to roll over into using migrate. Once in a more stable process, I can run something like hashdump to get a list of users and password hashes.  
 Text

Description automatically generated

After retrieving a hashdump, I could easily run these through John the Ripper and using the advanced and publicly available rockyou.txt dictionary, find out that they Administrator’s password isn’t actually all that secure at all, as it is “Passw0rd!”.   
  
Additionally, I can search directories and find files that are not intended for my eyes using the command “search -f \*secret\*” and “search -f \*recipe\*”.

Text

Description automatically generated

Text, website

Description automatically generated

Once the file location is found, I can easily download these files onto my own machine using the download command, as such:

Text

Description automatically generated

Once these files are on my own machine, I can peek into them and see all sorts of information I was not intended to be privy to.  
Text

Description automatically generated

There are several other things I could do on this machine remotely after gaining access via the Icecast Header exploit, but they don’t fall under this scope; therefore, this concludes my findings.

# Recommendations

In order to protect port 8000, GoodSecurity would like to recommend employing a reverse proxy in front of it to prevent unwanted access from the Internet. As this exploit is effective on Icecast versions 2.0.1 and below, updating to the latest version should prevent this specific exploit from being used. We would also strongly recommend keeping all your software up to date to ensure the latest security updates are applied so they will be less susceptible to exploitation.

Furthermore, GoodSecurity would also highly recommend that the Administrator change his password to something much less vulnerable, and to enable a more stringent password policy that requires much more complex passwords that can’t be easily found in a dictionary list.