**GoodSecurity Penetration Test Report**

[**sheapadilla2510@protonmail.com**](mailto:YOURNAMEHERE@GoodSecurity.com)

**April 5, 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, 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

Text

Description automatically generatedif

**Vulnerability Exploited**:

Icecast Header Overwrite/Icecast HTTP Header Buffer Overflow

**Vulnerability Explanation**:

The Icecast application running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can **remotely gain control of the victim’s system** by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

Some remote action that can be executed are:

* File discovery and exfiltration
* Key logging and screen capture
* Privilege escalation to Administrator

The other exploits that were found in the system were:

* exploit/windows/local/keext\_service
* exploit/windows/local/ms16\_075\_reflection

**Severity**:

Critical 10.0!!!

**Proof of Concept**:

Step 1:

Perform a service and version scan using Nmap to determine which services are up and running, however, started with the inconfig then did general Nmap on 192.168.0.0/24, then did an nmap on 192.168.0.20 and finally ran the nmap -sV -p 8000 192.168.0.20

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Step 2:

From the previous screen, you can see that the Icecast service is running, therefore I ran the searchsploit icecast to search for any icecast exploits:

Text

Description automatically generated

Step 3:

The next step was to start Metasploit and search for the icecast module and load it for use, I started with the msfconsole command the moved to the search icecast command and then used 0 for the exploit and checked the options.

Graphical user interface, text

Description automatically generated

Step 4:

Set the RHOST to the target machine and exploited it, I started with set RHOSTS 192.168.0.20 command and followed up with the exploit command.

Text

Description automatically generated

Text

Description automatically generated

Step 5:

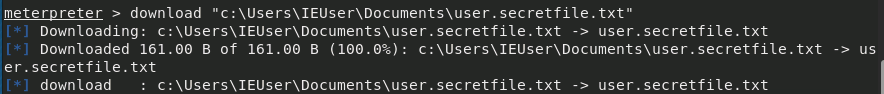
Did a search for the secretfile.txt on the target by running the meterpreter > search -f \*secret\*

Text

Description automatically generated

Step 6:

Upon completion of the previous step I downloaded the file and put it into the necessary folder. I then did an ls and found that the file had been placed where it needed to go.



Graphical user interface, text

Description automatically generated

Step 7:

Next we searched for the receipe.txt on the target by running meterpreter > search -f \*receipe\*.

Step 8:

Upon competition of the previous step I downloaded the file and put it into the necessary folder. I then did an ls and found that the file had been placed when it needed to go then ran a cat to get the necessary message which was:

“Put the lime in the coconut and drink it all up!”

Text

Description automatically generated

Step 9:

Finally searched for the enum file then ran a meterpreter post script that enumerated all logged on users with the

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Bonus Step 3:

Text

Description automatically generated

Bonus Step 4:

Text

Description automatically generated

Bonus Step 5:

Text

Description automatically generated

# **Recommendations**

The Icecast exploit is an old vulnerability that can be fixed with a patch by installing the latest version of this and all other software.

Would highly suggest that GoodCorp:

* Encrypt all files/folders that you want to keep a secret
* Enable windows firewall with rules to only explicitly allow traffic on needed ports.