GoodSecurity Penetration Test Report

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

7/15/2021

# 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

Vulnerability Exploited:

The module used in this exploit is a Buffer Overflow in the header parsing of Icecast version 2.0.1.

Vulnerability Explanation:

With a buffer overflow, I was able to access executable code and rewrite it to allow me into the system and take control of it. I was able to look at a download private files from your machine.

Severity:

A buffer overflow is pretty severe vulnerability because it allows a malicious attacker to access the system and basically take it over, they would be able to do things from steal secrets to completely take over the system.

Proof of Concept:

To find these exploits I first did a scan using `nmap -sV 192.168.0.20`

to find out what services and versions were being used.

Text

Description automatically generated

Text

Description automatically generated

After finding out what version of icecast was in use I was able to search for exploits in Metasploit. From there I was able run theexploit and set the host ip to the target maching and start searching for secret files and download them.

Text

Description automatically generatedText

Description automatically generated

Finally after successfully getting the files I was looking for I ran `exploit\_suggester` to find other vulnerabilities that could be exploited.

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generated

# Recommendations

One recommendation would to be to upgrade to version 2.0.2, version 2.0.1 is known to have this exploit that was fixed with upgrading to 2.0.2.