GoodSecurity Penetration Test Report

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

3/16/2022

# 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:

CVE-2004-1561

Vulnerability Explanation:

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

In short, is possible to execute remote code simply using the normal HTTP request plus 31 headers followed by a shellcode that will be executed directly without the need of calling/jumping to registers or addresses or using other annoying techniques.

Severity:

In your expert opinion, how severe is this vulnerability? High, It allows the attacker to remotely take over the system without having user credentials

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

Exploit to run

Text

Description automatically generated

Find secretfile.txt on MSEDGEWIN10

Text

Description automatically generated

Find recipe.txt on MSEDGEWIN10

Text

Description automatically generated

Enumerating All Users

Text

Description automatically generated

# Recommendations

What recommendations would you give to GoodCorp?

Either upgrading to the latest version of icecast or replace the application with something that is not vulnerable.