GoodSecurity Penetration Test Report

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

03/27/2021

# 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:**

Icecast HTTP Header Buffer Overflow

8000/tcp open http Icecast streaming media server

**Vulnerability Explanation:**

This vulnerability exploits a buffer overflow in icecast’s header parsing. By sending 31 HTTP headers you will cause a write one error past the end of a pointer array. However this only effects Windows with 32-bit architecture. Using this exploit will overwrite the saved instruction pointer. With various Linux distributions, using this same vulnerability is not necessarily an option or it overwrites nothing important. This exploit has a limited number of uses, due to its leveraging of ExitThread(). Every time this is used, icecast will not decrement the thread counter and therefore think it’s still in use. Therefore, every time your payload exits, the counter will be remain incremented. Eventually the threadpool limit will be maxed out. So you can only use this exploit as many times as there are remaining threadpool options.

**Severity:**

I’d give it an NVD CVSS Version 3.1 rating of 7.2.

Graphical user interface

Description automatically generated

IBM has some differing Base Score Metrics and they can be found at the following link: <https://exchange.xforce.ibmcloud.com/vulnerabilities/17538>

According to NVD CVSS Version 2.0 ratings, this is a 7.5.

<https://nvd.nist.gov/vuln/detail/CVE-2004-1561>

**Proof of Concept:** See <https://github.com/vjoh/GTPE-HW17/blob/main/README.md>.

# Recommendations

Recommend that GoodCorp ensures all versions of Icecast running on their network are versions 2.0.2 or later.