GoodSecurity Penetration Test Report

[tim.jambois@GoodSecurity.com](mailto:tim.jambois@GoodSecurity.com)

1/11/2021

# 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 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:

MSEDGEWIN10

Vulnerability Exploited:

Icecast

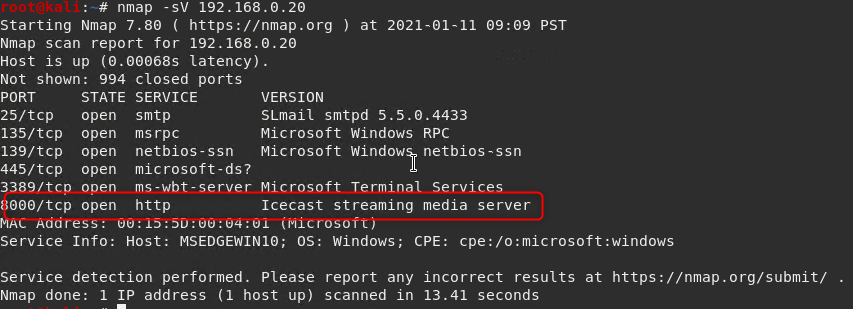
Vulnerability Explanation:

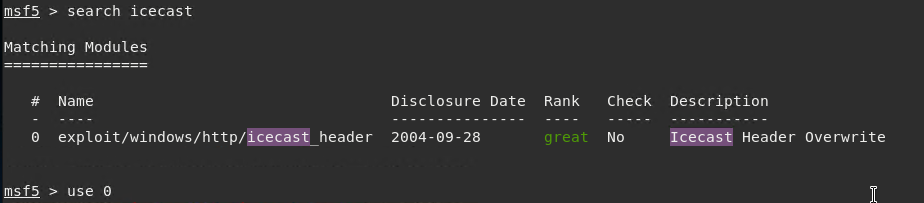
This exploit uses a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won't be decremented. This means for each time your payload exits, the counter will be left incremented

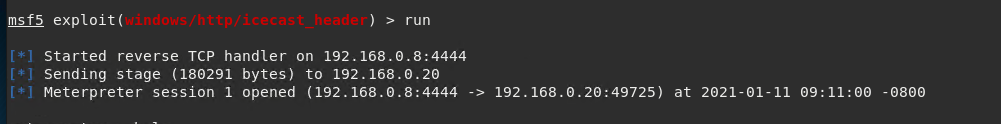
Severity:

Eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.

Proof of Concept:







# Recommendations

To remedy this potential exploit, it is my suggestion that Icecast be upgraded to 2.0.2 or later. Regular scan and maintenance of end users systems should be performed here after. This will ensure availability with all applications available.