GoodSecurity Penetration Test Report

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

07/17/2021

# 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\_header

Vulnerability Explanation:

Icecast\_header (See NIST’s National Vulnerability Database CVE-2004-1561) exploits a buffer overflow vulnerability in the header of Icecast versions 2.0.1 and earlier. The vulnerability is exploitable on windows machines and not linux-based machines, and fools Icecast into thinking the thread is still in use and consequently the thread counter is not decremented. This exploit can be run multiple times until the system threadpool limit reaches the maximum.

Severity:

NVD lists the Icecast header exploit as a 7.5 in the Common Vulnerability Scoring System (CVSS) making this a dangerous exploit allowing near full control access to a targeted machine.

Proof of Concept:

-The first step was conducting a service scan of the target machine using nmap, which shows open and running services. After gathering this information, SearchSploit was used to see if the Icecast Streaming Media Server had exploitable weaknesses:

Text

Description automatically generated

-The second step was to use Metasploit’s icecast module to exploit the buffer overrun on the target machine:

Text

Description automatically generated

-The third step was to Exploit the target machine, search for the flagged files, and download the recipe file:

Text

Description automatically generated

-Finally, additional access to the target machine was demonstrated by gathering a list of Users on the machine and some specific SystemInfo on the machine:

Text

Description automatically generated

Text

Description automatically generated

# Recommendations

The vulnerability would be closed by patching the program to a current version of the application that closes the exploit. Routine patching of programs on all enterprise machines is a good security practice that should be followed.

Plain-text files containing passwords should also not be stored on machines. If necessary, encrypted applications such as LastPass, Keepass, or NordPass are encrypted tools that can be used for storing passwords.

Routine scanning of open network ports on high priority machines should also be performed to check as new vulnerabilities arise.