GoodSecurity Penetration Test Report

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

July 7, 2020

# 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 Overwrite (exploit/windows/http/icecast\_header)

Vulnerability Explanation:

It is reported that the Icecast server with versions 2.x up to 2.0.1 are susceptible to a buffer overflow vulnerability. This issue is due to a failure of the application to properly enforce boundary conditions when dealing with user-supplied input data. By Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable). 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, and eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.   
  
This vulnerability allows for remote code execution in the context of the Icecast server.  
  
It is reported that this vulnerability is only exploitable to execute remote code on Microsoft Windows platforms. This buffer overflow affects all platforms, however it is only exploitable if a sensitive address is located adjacent to the affected buffer. On other platforms, denial of service or code execution may be possible, but this has not been confirmed.

Severity:

The severity of this vulnerability is high (CVSS Score 7.5) since it impacts all confidentiality, integrity and availability.

Proof of Concept:

1. Using Nmap command that performs a service and version scan against the target. A screenshot of text

   Description automatically generated
2. Using SearchSploit to show available Icecast exploits

A screenshot of a cell phone

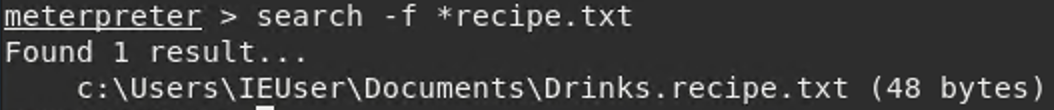
Description automatically generated

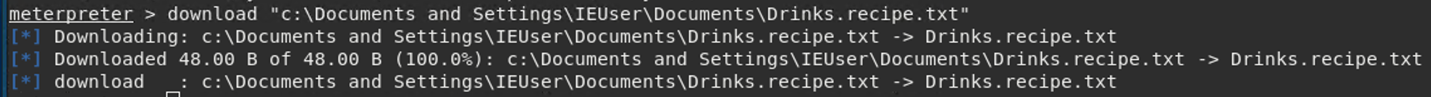
1. Using Metasploit to search for the Icecast module and load it for use

A screenshot of a cell phone

Description automatically generated

1. Run the Icecast exploit and perform remote code execution and exfiltrates files





# Other Vulnerabilities

# **MS16-075**

The vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.

# Recommendations

Upgrade all the icecast server to at least version 2.02