GoodSecurity Penetration Test Report

[USHANY@GoodSecurity.com](mailto:USHANYKANAGENDIRAN@GoodSecurity.com)

May 7, 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: exploit/windows/http/icecast\_header

Icecast Header Overwrite

Vulnerability Explanation:

* Attack type: Buffer Overflow
  + The buffer overflow exploit in Icecast is a flaw in the program where an attacker is able to overwrite its memory. This flaw will allow an attacker to execute code on the program to gain remote access of the target system.

Severity:

In my expert opinion, this vulnerability is highly severe. This vulnerability allows unauthorized person to access sensitive company information remotely. Additionally, it was found that the attacker can further escalate their privileges through this vulnerability.

Proof of Concept:

1. First an Nmap scan was conducted to see what services are running and on what ports.
   1. Services found: Icecast, Microsoft Terminal Services, netbios-ssn, RPC, SLmail smtpd

Text

Description automatically generated

1. Searchsploit was used on Icecast to determine exploits in the service

Text

Description automatically generated

1. Metasploit was then used to load the Icecast module
   1. RHOST was set to 192.168.0.20 (target machine)
   2. The exploit was then run on the target machine

Text

Description automatically generated

Text

Description automatically generated

1. Once remote access to the target machine was achieved, I was able to search, view and download files from the target machine

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, application

Description automatically generated

1. I was also able to view other local exploits on the system

Text

Description automatically generated

1. Lastly, I was able to open a meterpreter shell and view the system information of the target machine

Text

Description automatically generated

Text

Description automatically generated

# Recommendations

In order to prevent GoodCorp from being attacked through this vulnerability, they should make sure that the Icecast service is up to date. The vulnerability found above affects Icecast versions 2.0.1 and older.