GoodSecurity Penetration Test Report

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

05/04/2022

# 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 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 : 8000/tcp open http Icecaset streaming media server.

Vulnerability Explanation:

The Icecast version 2.0.1 or older running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim’s system by overwriting the memory on the system. To exploit this flaw, an attacker needs to send 32 HTTP headers to the remote host to overwrite a return address on the stack.

Severity:

Remote code execution in ICECAST server has Very HIGH CRITICAL Risk. CVVS Score greater than 8.0

Proof of Concept:

1. Run : nmap -sS -v 192.168.0.20

Text

Description automatically generated

1. Search for an Icecast exploitText

   Description automatically generated
2. Start Metasploit:Text

   Description automatically generated
3. Search for the Icecast module and load it for use.Text

   Description automatically generated
4. Set the RHOST on the target machine and the the exploitText

   Description automatically generated
5. Meterpreter Session opens and search for the file “Secretfile” and “receipe” file.Run the command to extract the file.Text

   Description automatically generated

Bonus: A. Run a Meterpreter postscript that enumerates all logged on users.

B. Open a Meterpreter shell and gather system information for the target

C. Run the command that displays the target's computer system information:

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

# Recommendations

The Icecast Exploit is an old vulnerability that can be fixed with patch. Installing newer version is highly recommended.