GoodSecurity Penetration Test Report

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

Friday, July 17, 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:

Actual name of the machine

Vulnerability Exploited:

exploit/windows/http/icecast\_header

Vulnerability Explanation:

Icecast Header Overwrite

This module exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma. 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.  
  
<https://www.rapid7.com/db/modules/exploit/windows/http/icecast_header>

For more info please refer to <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1561>

Severity:

The vulnerability is ranked as very severe since the system can be compromised within a few minutes.

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

There should be a separate finding for each vulnerability found!

# Recommendations

What recommendations would you give to GoodCorp?

Remove the icecast server from the machine and switch to amore secure alternative.