GoodSecurity Penetration Test Report

LaurenEvans[@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

APRIL 6, 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:

The remote web server runs Icecast version 2.0.1 or older. Such versions are affected by an HTTP header buffer overflow vulnerability that may allow an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process.

Severity:

In your expert opinion, how severe is this vulnerability? Critical, The exploit has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.

Proof of Concept:

* Run the Nmap command that performs a service and version scan against the target.
* Run the SearchSploit commands to show available Icecast exploits.
* Recommendations

What recommendations would you give to GoodCorp?