GoodSecurity Penetration Test Report

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

04/11/2022

Table of Contents

[1.0 High-Level Summary 3](#_Toc100605073)

[2.0 Findings 4](#_Toc100605074)

[3.0 Recommendations 11](#_Toc100605075)

[4.0 Resources 11](#_Toc100605076)

# 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

Vulnerability Explanation:

Icecast allows for a buffer overflow exploit. This exploit allows the attacker to send HTTP headers remotely to gain control of a victim’s system by overwriting the memory.

Severity:

Critical 10.0

Proof of Concept:

Locating the IP address:

Text

Description automatically generatedText

Description automatically generated

Pinging DVW10 to check for response.

Text

Description automatically generated with medium confidence

Ran nmap scan to check for any vulnerabilities on the DVW10 machine. The scan came back with the Icecast Streaming media server.

Text

Description automatically generated

The DVW10 machine within Icecast the following changed when running the nmap scan.

Graphical user interface

Description automatically generated with low confidence

Searching for Icecast Exploits.

Graphical user interface, text

Description automatically generated

Bringing up the meterpreter session.

Graphical user interface, text

Description automatically generated

Then had to set the options for RHOST.

Text

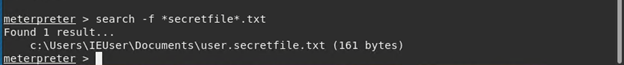
Description automatically generated

Running the exploit.

Text

Description automatically generated

Finding secretfile.txt and recipe.txt.



Exfiltrating the files.

Text

Description automatically generated

Uncovering additional vulnerabilities.

Text

Description automatically generated

Using the exploit suggester uncovered two more vulnerabilities.

exploit/windows/local/ikeext\_service

exploit/windows/local/ms16\_075\_reflection

Enumerating Logged on users.

Text

Description automatically generated

System information from the meterpreter shell for DVW10 machine.

Text

Description automatically generated

The system information from the meterpreter shell.

A picture containing text

Description automatically generated

# Recommendations

The Icecast Header Overwrite was the highest priority vulnerability out of the three found. The recommendations I suggest would be to upgrade to the latest version of Icecast which is 2.0.x or later.

IKEEXT\_Service and ms16\_075 exploits are harder to expose than the Icecast vulnerability. These two vulnerabilities are potentially dangerous and still pose a threat. To prevent an attack my recommendations are to make sure you have the latest updates and patches.

Updating the system regularly mitigates the risk of any potential threats and attacks on the system. Updating regularly (monthly) at minimum would be considered best practice and would be the first place to start for increasing security on the system and network.

# Resources

***Icecast is free server software for streaming multimedia***

<https://www.icecast.org/>

***Nessus Plugin ID 14843. (2004, 09 28). Icecast HTTP Header Processing Remote Overflow, 1.24. Retrieved from Tenable:***

https://www.tenable.com/plugins/nessus//14843