**GoodSecurity Penetration Test Report**

[NicoleTKemp@GoodSecurity.com](mailto:NICOLETKEMP@GoodSecurity.com)

Tuesday, 5th April 5, 2022

Table of Contents:

Title 1

Table of Contents2

1.0 High-Level Summary 3

2.0 Findings4

3.0 Recommendations5

References6

# 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 (specific exploit used `Exploit/windows/http/icecast\_header`)

Vulnerability Explanation:

The Icecast application contains a buffer overflow vulnerability that allows an attacker to take remote control of the victim's machine by overwriting memory with the Icecast flaw, which writes past the end of a pointer array. This is a massive vulnerability. Buffer overflow attacks give attackers the ability to harm files and reveal confidential information. While buffer overflow attacks are most often associated with system crashes, they can potentially result in far bigger hostile behavior. Finally, this vulnerability may result in data loss or theft, ransomware assaults, or serve as a gateway to a range of other attack vectors.

Severity:

Critical! YOU SHOULD BE FIXING THIS NOW.

Proof of Concept:

Please see readme file. It can be used as a detailed guide on what commands you need to enter as well as screenshots provided to show results: <https://drive.google.com/file/d/1RsKsY8-74HbDJ44xXYcD66bpc5vNr0AI/view?usp=sharing>

# Recommendations

I recommend upgrading your Icecast to version 2.0.2 or later first. Because the Icecast Header Overwrite vulnerability is the most serious of the discovered flaws, The IKEEXT and ms16075 exploits are more difficult to find than the Icecast vulnerability, but they could be more dangerous. Regular system updates and the installation of the necessary patches will be required to keep your system secure against future vulnerabilities.

Monthly patch updates are regarded as best practice and would be a good place to begin. Finally, I recommend that you apply the available patches to address both vulnerabilities in order to prevent an attack in which the attacker can escalate their privileges.

# 4.0 References

Reference list

InfosecMatter. (2020). *Icecast Header Overwrite - Metasploit - InfosecMatter*. [online] Available at: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/icecast\_header [Accessed 7 Apr. 2022].

Rapid7. (n.d.). *Icecast Header Overwrite*. [online] Available at: https://www.rapid7.com/db/modules/exploit/windows/http/icecast\_header/ [Accessed 7 Apr. 2022].

www.tenable.com. (n.d.). *Icecast HTTP Header Processing Remote Overflow*. [online] Available at: https://www.tenable.com/plugins/nessus/14843 [Accessed 7 Apr. 2022].