GoodSecurity Penetration Test Report

RobertForee[@ScenarioLab.com](mailto:robforee@ScenarioLab.com)

10/25/2021

# 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.

exploits a buffer overflow

Nessus scan of [IEUser@MSedgeWin10](mailto:IEUser@MSedgeWin10) results

Discovered 9 vulnerabilities of medium severity.

* 17592 - Icecast XSL Parser Multiple Vulnerabilities (OF, ID)
* 63155 - Microsoft Windows Unquoted Service Path Enumeration
* 57608 - SMB Signing not required
* 51192 - SSL Certificate Cannot Be Trusted
* 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
* 57582 - SSL Self-Signed Certificate
* 104743 - TLS Version 1.0 Protocol Detection
* 121010 - TLS Version 1.1 Protocol Detection
* 58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Onl

# Findings

Machine IP: **192.168.0.20**

Hostname: **MSEDGEWIN10**

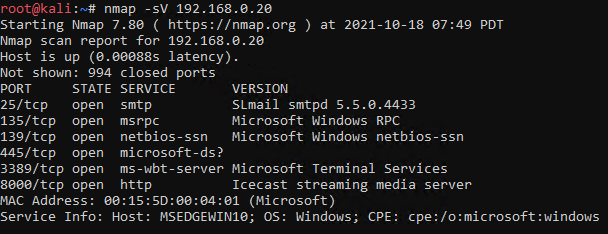
Vulnerability Exploited: **Icecast Header Overwrite**

Vulnerability Explanation: **This module exploits a buffer overflow in the header parsing of Icecast versions 2.0.1 and earlier**

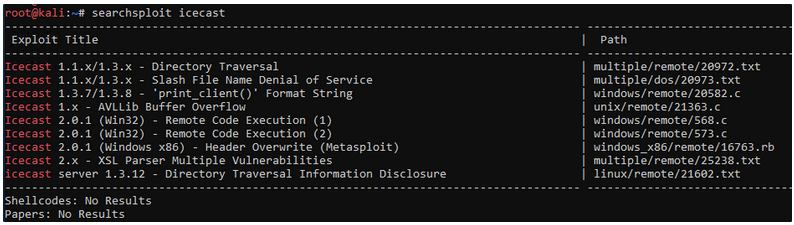
Severity: **This vulnerability is SEVERE**

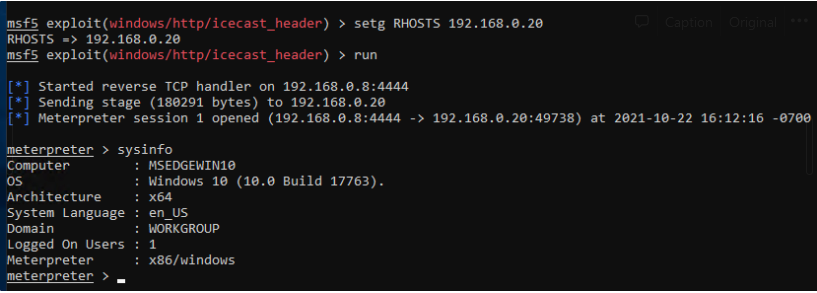
Proof of Concept: **Icecast was exploited via the XSL parser.**

Scan of host finds Icecast running

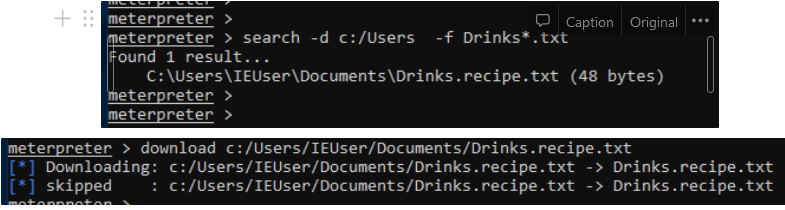


SearchSploit identifies multiple exploits of Icecast v 1 and v2

Metasploit was able to start a reverse shell



The exploit allowed exfiltration of company secrets.



# Recommendations

Given that this is the CEO’s computer and it contains company secrets, we recommend GoodCorp make the following changes to MSEDGEWIN10.

In general remove all unnecessary applications, maintain current software versions, close all unnecessary ports and enable strict password policies.

# add patches to update icecast app, port 6812  
# Seattle Lab Mail (http 180)  
# Seattle Lab HTTP Server/1.0 port 180, 3404

Add patches or remove icecast app (v 3.x or greater)

Add patches or remove freeFTPd (v1.0.13 or greater)

Eliminate unquoted service path violations by Seattle Lab Mail and Free FTP applications.

restrict or close ports 135 and 445 disallowing file and printer sharing

Downgrade IEUser from Administrator to user privileges

Set IEUser maximum password age 42

Delete disabled accounts Administrator and Guest

Prevent access via ICMP to timestamp request

Disable LLMNR name resolution

Prevent anonymous lookups of the host SID by setting RestrictAnonymous regestry setting