|  |
| --- |
| GoodSecurity |
| Penetration Test Report |
| 30 September 2021 |

|  |
| --- |
| Prepared By:  **David Chen**  https://github.com/chenperfidelis/ |

# 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans’ computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on Hans’ computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Scope

The scope of this engagement is limited to the CEO's workstation only. You are not permitted to scan any other IP addresses or exploit anything other than the CEO's IP address. The CEO has a busy schedule and cannot have the computer offline for an extended period of time. Therefore, denial of service and brute force attacks are prohibited. After you gain access to the CEO’s computer, you may read and access any file, but you cannot delete them. Nor are you allowed to make any configurations changes to the computer.

# Findings 1

## Machine IP:

192.168.0.20

## Hostname:

MSEDGEWIN10

## Vulnerability Exploited:

Icecast Header Overwrite (CVE-2004-1561)

## Vulnerability Explanation:

This is a buffer overflow vulnerability. The module exploits a buffer overflow in the header parsing of Icecast by sending 32 HTTP headers causing it to write past the end of the pointer array by one. On a Windows OS, this overwrites the save instruction pointer. By using ExitThread(), it leaves Icecast thinking the thread is still in use therefore the thread counter does get decremated.

## Severity:

High Severity – Once exploited, attackers are able to explore and exfiltrate files

## Proof of Concept:

Performed a scan with Nmap on target computer  
Text

Description automatically generated

Located open port 8000  
Version scan determined the service on port 8000 is Icecast streaming media server



Searchsploit located possible exploits  
Text

Description automatically generated

Load Icecast Header Overwrite exploit and set target  
Text

Description automatically generated

Confirmed options set Text

Description automatically generated

Run exploit, drop system shell Text

Description automatically generated

# Findings 2

## Machine IP:

192.168.0.20

## Hostname:

MSEDGEWIN10

## Vulnerability Exploited:

Seattle Lab Mail 5.5 POP3 Buffer Overflow (CVE-2003-0264)

## Vulnerability Explanation:

An unauthenticated buffer overflow vulnerability in the POP3 server of Seattle Lab Mail v5.5 when sending an exceptionally long password.

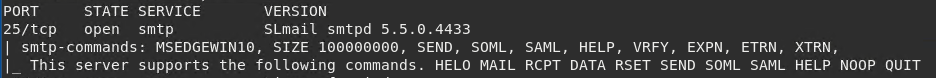
## Severity

High – able to obtain administrator shell

## Proof of Concept:

Performed a scan with Nmap on target computer  
Text

Description automatically generated

Noted open port 25 running service: SLmail smtpd 5.5.0.4433  
****

Search exploits  
**Graphical user interface, text, website

Description automatically generated**

Set remote port and host  
Text

Description automatically generated

No POP3 sessions running at time of testing, however vulnerable version of SLMail  
**Text

Description automatically generated**

# Recommendations

* Update to the latest version of Icecast where the vulnerability has been addressed
* Set up firewall to only allow approved source IP address access to Icecast port 8000
* Update Seattle Lab Mail (SLmail) to the latest patched version
* Ports 139 and 445 (SMB share) should be blocked by firewall if SMB file is not required by the CEO’s PC
* 3389 (Remote Desktop Protocol) port should be blocked or restricted to authorised IP addresses if required.