

Contents

[High-Level Summary 3](#_heading=h.gjdgxs)

[Findings 3](#_heading=h.30j0zll)

[Recommendations 9](#_heading=h.1fob9te)

[Sources 9](#_heading=h.3znysh7)

# 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.

# Findings

**Machine IP:**

**192.168.0.20**

**Hostname:**

**MSEDGEWIN10** (it’s a Windows machine)

**Vulnerability Exploited:**

Icecast Header - exploit/windows/http/icecast\_header

**Vulnerability Explanation:**

This module exploits a buffer overflow in the header parsing of icecast. This exploit was discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on Linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable).

This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won’t be decremented.

This means for each time your payload exits, the counter will be left incremented, and eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.

**Severity:**

Medium.

**Proof of Concept:**

Used nmap to check the services and version of the victim machine to check open ports. We can see that the Icecast service is running.

A close up of text on a black background

Description automatically generated

Used the searchsploit tool to search for Icecast exploits:

A screenshot of a cell phone

Description automatically generated

Once I could see the available exploits, I started Metasploit and searched for the Icecast module. Once I found the exploit module (exploit/windows/http/icecast\_header), I ran a command to use the Icecast module and set the remote host to the victim’s IP address (192.168.0.20). I then ran the exploit:

A screenshot of a cell phone

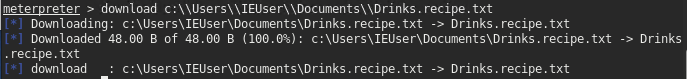
Description automatically generated

By running the exploit, I started Meterpreter, which I used to find the secretfile.txt and recipe.txt files:

A screenshot of a cell phone

Description automatically generated

I then used the download command to extract the recipe.txt file:



Using Meterpreter, I ran a post-script to enumerate all logged-on users:

A screenshot of a cell phone

Description automatically generated

I then opened the Meterpreter shell and gathered system info on the target:

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

I used the exploit suggester to see if there were any other vulnerabilities:

A close up of a logo

Description automatically generated

**Vulnerability Exploited:**

exploit/windows/local/ikeext\_service

**Vulnerability Explanation:**

This module exploits a missing DLL loaded by the 'IKE and AuthIP Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts automatically in default installations of Vista-Win8. It requires an insecure bin path to plant the DLL payload.

**Severity:**

Medium

**Vulnerability Exploited:**

exploit/windows/local/ms16\_075\_reflection

**Vulnerability Explanation:**

Module utilizes the Net-NTLMv2 reflection between DCOM/RPC to achieve a SYSTEM handle for elevation of privilege. Currently the module does not spawn as SYSTEM, however once achieving a shell, one can easily use incognito to impersonate the token.

**Severity:**

Windows 7 and XP more at risk than later versions.

# Recommendations

For the Icecast exploit:

1. Have a proper stateful firewall in place and make sure it is up to date.
2. All computer services and systems should be up to date, including update patches.
3. Daily Log monitoring on firewalls, routers, and IDS/IPS.
4. Use the latest Icecast service version.

For the Ikeext exploit:

1. To avoid exploitation of this weakness developers should use full path when using an external library and should not rely on default search order of DLL files.
2. When developing application for Windows systems use Microsoft recommendations to limit the attack surface.

For the NTLM exploit:

1. Apply relevant patches and keep the system up to date.

# Sources

* <https://www.rapid7.com/db/modules/exploit/windows/local/ikeext_service>
* <https://www.rapid7.com/db/modules/exploit/windows/http/icecast_header>
* <https://www.rapid7.com/db/modules/exploit/windows/local/ms16_075_reflection>