CS557 Project 4: Screen 4.5

Thomas Le Baron
Team 1010
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
tlebaron@wpi.edu

Brittany Lewis
Team 1010
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
bfgradel@wpi.edu

***Abstract*—**

I. Finding Screen

- **Progam:**
- **Exploit:**`/home/user/exploit.sh`
- **md5sum hash of the binary file:**
- **md5sum hash of the source file:**

II. Introduction

GNU Screen is a terminal multiplexer which allow the user to access multiple processes from an unique terminal. It is the shell version of a window manager. In 2017, Screen 4.5 presented a vulnerability allowing a user to get root privileges in the local machine running the program. In this work we show a proof of concept of how this vulnerability can be used to get root privileges.

III. Design

`/ect/` is a root-owned folder. Therefore, all its content is supposed to be owned by root and therefore is considered safe. `/etc/ld.so.preload` is a list of additional, user-specified, EFL shared libraries to be loaded before any others. Nevertheless, it is possible to create such a file if it doesn't already exist, and write in arbitrary libraries.

The vulnerability of GNU Screen 4.5 comes from the fact it opens the `ld.so.preload` file with root privileges without any verifications. With this, the library written in the file can be used to create a root-owned file, with arbitrary content and location. This second file can be a simple program with an `exec` instruction, sufficient to get a shell with root privileges.

IV. Implementation

A. Environment Creation

The Docker image does not need any configuration. For isntance, ASLR is kept enabled.

The program exploited is GNU Screen 4.5. We followed the usual step to install a software on a linux system from a compressed file. After uncompressing the software folder, we run `./configure`, `make` and `make install`.

B. Exploit Construction

The exploit has three parts.

- First we create the library and the exploit file. The library corresponds to the lines 11-20 of the exploit. Its job is to give the exploit file the root privileges needed. It also unlink the `/etc/ld.so.preload` file so that the library is not called more than once. The exploit file simply get root privileges and execute `execvp("bin/shh")`. It corresponds to the lines 25-32.
- Then we add the library to the `/etc/ld.so.preload` file. Done line 39, it can be only done if this file doesn't exist in the first place.
- Second we run Screen again. Before running, all the libraries in the `ld.so.preload` will do so. Since Screen has root privileges, then the library added will execute, giving the exploit file all the privileges needed. Once done, we simply run the exploit file with `/tmp/rootshell`.

V. Exploitation

The proof of concept can be run following:

- If logged as root, change your permission to user with `su - user`
- You should already be in the `home/user/` folder. If not, execute `cd home/user/`
- The exploit is the `exploit.sh` file. Simply execute it with `sh exploit.sh`
- Enjoy your new privileges.

VI. Conclusion

A. Comments on the vulnerability

It seems that the issue with GNU Screen 4.5 is not a code bug. We did not use code vulnerabilities and techniques we learnt in the CS557 classe to get privilege escalation. The main issue with Screen is a design mistake. The devlopers of the softwares did not conceive that opening the logfiles in root privileges could be used to create root-owned files.

B. Reference

The proof of concept used in this project is published at `https://www.exploit-db.com/exploits/41154/`.