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

The vulnerability of GNU Screen 4.5 comes from the fact that logfiles are opened with root privileges. Doing so allow any user to create a root-owned file with arbitrary content. A simple program with an `exec` instruction is sufficient to get the control of the 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. The program is not modified, but we added manualy the reference of the program to the `usr/bin/` folder. Doing so allows the exploit file to run the Screen program without having to give its address.

B. Exploit Construction

The exploit has two parts.

- First we need to create the logfile. Opened with root privileges, the content of it is not checked but can be entirely written by the user. In the proof of concept, it concerns the lines 11-20. It simply gives a second file the permissions needed to be executed as root.
- The second file get the root permission from the first one. Its content suits the need of the attacker. In our case, we simply set the current user permissions to root and execute the `execvp("/bin/shh")` instruction, which gives a shell with root privileges. This second file is described lines 25-32.

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/folder`
- 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/`.