

Name: cPanel
Vendor URL: <http://www.cpanel.net>
Author: Karol Więsek <appelast@drumnbass.art.pl>
Date: July 31, 2004

Issue:

cPanel allows logged in users to change ownership of any file to their uid:gid.

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 page extensions. It is done with effective uid of system administrator (root). During this process is created special *.htaccess* file, and then it is chown() to target user. Attacker could link *.htaccess* to any file in the same partition, thus it will be chown()'ed.

Exploit:

To exploit this vulnerability just link file you want to grab to *.htaccess* in users public_html, and execute installation of frontpage extensions.

Tested on cPanel 9.4.1-RELEASE-64, and confirmed vulnerable.