

Name: cPanel  
Vendor URL: <http://www.cpanel.net>  
Author: Karol Więsek <appelast@drumnbass.art.pl>  
Date: July 19, 2004

### **Issue:**

cPanel backup feature allows logged in users to read any file, including they have not permission to read to.

### **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 backup system allows attacker to insert into archive and then download files, that he does not have permission to access. System backup follows hard links ( thus it is only possible on the same partition ) and copies it into tar.gz archive. Attacker could use php ( normal www ) to link file in his public\_html to for example /etc/shadow, and then execute backup ( *Backup -> Generate/Download a Full Backup* ).

### **Exploit:**

To exploit this vulnerability just link file you want to grab to some file in \$HOME and execute backup.

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