
Subject: Re: OpenVZ Web Panel & Sicherheit
Posted by [curx](#) on Wed, 15 Dec 2010 13:50:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

Tach auch,

meinste das Panel:
<http://code.google.com/p/ovz-web-panel/>

und die Sicherheit des Ruby hw-daemon.rb (daemon), welcher per XML-RPC am Port 7767 (default) lauscht ?

beim ersten Durchblick unter:
<http://ovz-web-panel.googlecode.com/svn/trunk/utils/hw-daemon/hw-daemon.rb>

macht dieser via exec auch nur eine Befehlsausführung und muss daher für OpenVZ erstmal unter root laufen.

"Bauchschmerzen":

* die "OpenVZ" commands werden beim "Daemon" nicht geprüft, daher könnte unter Umständen hier Befehle als root abgesetzt werden
Workaround :dem Dienst einen eigenem User verpassen, die OpenVZ nur über sudo oder wrapper erreichbar machen, sollte hier schon einmal für eine weitere Sicherheitsstufe sorgen. Zumindestenz werden Befehle nicht ausgeführt, die man(n) auch für OpenVZ nicht braucht.

* TLS des Servers hw-daemon wäre gut, da hier das PW/Secret unverschlüsselt übermittelt wird, evtl. sogar der rootpw der CT root Users, wenn entsprechend übermittelt/gesetzt wird.

* default Einstellung der \$SERVER_ADDRESS = "0.0.0.0", würden ich eher auf "127.0.0.1" setzten und wenn wirklich über das Netz dann nur TLS und mit via IPTables "absichern"

... so mal eben kurz beim Drüberblicken, ach ja und die Webbrick-Http Interface Schnittstelle bisher nicht weiter durchgesehen.

Gruß,
Thorsten
