Subject: OpenVZ Web Panel & Sicherheit
Posted by shamu on Wed, 15 Dec 2010 10:24:01 GMT
View Forum Message <> Reply to Message

Hallo zusammen,

gibt's hier im Forum jemanden, der sich mit dem dem OpenVZ Web Panel und dabei insbesondere mit dem Thema Sicherheit bei den aufgebauten Verbindungen zum hw-daemon und zur sqlite DB auskennt?

Habe dazu zwar schon ein ausführliches Posting auf Englisch geschrieben, aber das ist vom Moderator noch nicht quer gelesen und freigegeben.

Natürlich klappt es in der Muttersprache immer etwas besser mit der Kommunikation, darum meine Frage auch hier im deutschen Zweig.

Greetinx

shamu

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-daemo n/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 ereichbar machen, sollte hier schon einmal für eine weitere Sichheitsstufe 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

Subject: Re: OpenVZ Web Panel & Sicherheit
Posted by shamu on Thu, 16 Dec 2010 07:42:03 GMT
View Forum Message <> Reply to Message

Hallo Thorsten,

vielen Dank erstmal für dein Reply, deine Empfehlungen und Hinweise!

Mein ursprünglicher Beitrag (auf englisch) ist übrigens jetzt von den Forum-Admins abgenickt worden und online, darum verzichte ich hier darauf, alles nochmal auf deutsch wiederzugeben. Hier der Link: forum.openvz.org/index.php?t=msg&th=9250&start=0&amp ; (sorry für die umständliche Darstellung, aber Links sind in diesem Forum erst ab > 10 Beiträge erlaubt)

Einer der darauf bereits geantwortet hat, meinte ich solle mich an die Entwickler des Web Panels und nicht an dieses Forum wenden. Nur genau das ist aber mein Problem! Dort kannst du zwar neue Issues (Bugs melden, Modifikationen wünschen, etc.) eintüten, aber halt keine Fragen stellen. Und ein Forum speziell zum Web Panel habe ich noch nicht gefunden, darum mein Versuch hier.

Da ich kein Rubi-Entwickler und ein wenig lazy bin, hab' ich gedacht, ich frag' mal in diesem Forum, vielleicht haben andere ja bereits Erfahrungen mit dem Panel und seiner Security.

Nun ja, nachdem in einer der letzten c't ein Beitrag über die libvirt stand, werde ich mir die auch mal anschauen und versuchen rauszufinden, wie die mit dem Thema Security umgehen.

Greetinx

shamu

Subject: Re: OpenVZ Web Panel & Sicherheit
Posted by shamu on Fri, 17 Dec 2010 12:08:03 GMT
View Forum Message <> Reply to Message

Hallo Forum,

hier noch ein kurzes Feedback, wie ich die Sache (für mich) gelöst habe:

Bei Libvirt gibt es verschiedene Möglichkeiten, die Übertragung zu verschlüsseln. Allerdings bin ich doch wieder zum OpenVZ Web Panel zurückgekehrt, weil dabei wesentlich weniger Pakete installieren werden müssen und mir (persönlich) die Darstellung besser gefällt, was natürlich Geschmackssache ist.

Auch habe ich ein paar Sachen getestet, die Thorsten vorgeschlagen hat. Also dann:

0. Feedback vom Entwickler: Benutzt für die Verbindung zwischen Panel und hw-daemon nur sicher Netze (LAN, Intranet, etc.). Daher sind keine Security Features für die Kommunikation zwischen panel und hw-daemon implementiert.

1. Der hw-daemon agiert nur dann richtig, wenn er als root läuft - leider Unter einem anderen Benutzer gestartet führt der Access vom Panel aus zu keinen Ergebnissen bzw. zu Fehlermeldungen.

2. Habe ich auf dem hw node sowie auf dem Panel Server einen dummy-User mit stark eingeschränkten Rechten angelegt, der sich ausschließlich per ssh key authentication am hw node anmelden kann.

3. Wird die Verbindung zwischen Panel und hw node nun über ssh getunnelt, d.h. es sind keine zusätzlichen offenen Ports erforderlich amd hw node. Den hw-daemon lasse ich nur noch auf Port 127.0.0.1 lauschen. Die (lokale) Umleitung besorgt netcat.

4. Die ssh-Session wird nur on demand aufgebaut, d.h. vom panel-server aus via xinetd.

5. Erlaube ich dem dummy-User auf dem hw-node mit netcat nur noch den Zugriff auf den hw-daemon.

6. Habe ich den timeout des hw-daemon relativ kurz angesetzt.

Das war's. Ich denke, wer sich mit ssh, (x)inetd und nc ein wenig auskennt, kommt mit der oben skizzierten Lösung zurecht.

Greetinx

shamu

Subject: Re: OpenVZ Web Panel & Sicherheit

Posted by curx on Sun, 19 Dec 2010 18:34:43 GMT
View Forum Message <> Reply to Message

@shamu:

würdest Du (wenn möglich) im OpenVZ wiki (wiki.openvz.org) hierzu einen Eintrag machen, vielleicht hat jemand Bedarf für diese Konstellation.

Gruß,
Thorsten