Plesk: Plesk 10.2: Verschlüsseltes Passwort?

Einführung:

Vielen Admins ist die Datei `/etc/psa/.psa.shadow` unter Plesk bekannt und manchmal gefürchtet. Hier wurde das Admin-Passwort von Plesk im Klartext gespeichert. (Die Datei hat natürlich nur Leserechte für root.)

Dies erlaubte eine Vielfalt von Möglichkeiten. Z.B. war ein Fremd-Admin lediglich auf den Root-Zugang angewiesen und konnte sich den MySQL-Admin-Zugang und die Plesk-Daten selber auslesen. Auch so bequeme Zeilen wie:

```
mysql -uadmin -p`cat /etc/psa/.psa.shadow`
```

sind gerne als Shortcut (z.B. als "User-Command" in Kitty) abgelegt.

Seit Plesk 10.2 wird dieses Passwort nun "verschlüsselt". Dies soll die Server-Sicherheit erhöhen.

Allerdings merkt auch Parallels in den Release-Notes an, dass es bei Upgrades (z.B. von 10.1) zu Problemen kommen kann.

Details:
MySQL-Aufrufe

Angeblich soll der Aufruf von MySQL weiterhin genauso funktionieren.

Upgrade von älteren Versionen

Wie schon angedeutet, vermutet Parallels beim Wechsel von älteren Versionen Probleme. Daher verschlüsselt der Update-Manager diese Datei nicht. Wer hingegen Plesk 10.2 neu auf setzt bekommt diese Datei verschlüsselt.

Natürlich kann die Datei auch im Nachhinein verschlüsselt (und auch entschlüsselt) werden:

```
/usr/local/psa/bin/init_conf -encrypt-password
#bzw zum entschlüsseln:
/usr/local/psa/bin/init_conf -decrypt-password
```

Klartext-Passwort

Genauso ist weiterhin das Passwort im Klartext anzeigbar:

```
/usr/local/psa/bin/admin --show-password
```

Fazit

Plesk: Plesk 10.2: Verschlüsseltes Passwort?

Letztendlich fragt man sich, was das ganze soll?
Wo ist der Mehrwert an Sicherheit, der hier propagiert wird?
Schläft ein Server-Betreiber jetzt besser, nur weil das Admin-Passwort nicht im Klartext gespeichert wird, aber dennoch jederzeit anzeigbar ist?
Parallels behauptet in der Release-Note, dass es sich um ein "encrypted hash" handeln würde. Dies kann aber nicht sein, da Encrypted-Hashes nicht reversibel sind. Die o.g. Aufrufe zum wiederherstellen des Plaintext-Password bezeugen das Gegenteil.

Aus meiner Sicht ist dies reine Augenwischerei!

Eindeutige ID: #1408
huschi
2011-04-28 12:43