Debian Etch oder Lenny PATCH NOW Debian Etch oder Lenny PATCH NOW

2008-05-18 04:16 von Kelli (0 Kommentare)

Wer auf seinem (Game-)Server Debian Etch oder jünger einsetzt sollte diesen JETZT Patchen.

Durch einen Fehler in dem openssl Paket sind die SSH, OpenVPN etc.. Schlüssel erratbar. Betroffen sind alle openssl Versionen ab 0.9.8c-1 bis 0.9.8c-4etch3 bzw 0.9.8g-9 bei der unstable/testing Linie. Der Befehl "openssl version" gibt Auskunft über die aktuell installierte Version. Wer seine ssh Authorisierung über das eigentlich sichere Pubkey Verfahren erledigt ist ironischerweise am stärksten gefährdet.
Nach dem Update von openssl (apt-get update sollte es tun) müssen auch alle bisher erzeugten Schlüssel auf dem System ausgetauscht werden. ssh-keygen sollte dann für jeden nach dem September 2006[!] erzeugten Schlüssel pflicht sein.

Betroffen sind auch Debian Abkömmlinge wie Ubuntu etc..

[1] http://www.debian.org/security/2008/dsa-1576
[2] http://isc.sans.org/diary.html?storyid=4420
[3] http://www.heise.de/security/

Zurück