Sigurnosni nedostaci unutar programskog paketa OpenSSL

Otkriveni su sigurnosni nedostaci u programskom paketu **OpenSSL**. Otkriveni nedostaci su uzrokovani neispravnom provjerom **OSCP** odgovora i neispravnim radom **CBC** moda šifriranja. Potencijalnim napadačima je omogućeno izvođenje **DoS** napada i otkrivanje određenih informacija statističkom analizom.

Ove ranjivosti imaju oznake: **CVE-2013-0166**, **CVE-2013-0169** i **DSA-2621-1**.

Ranjivosti su ispravljene u paketu openssl verzije **0.9.8o-4squeeze14** za **Debian squeeze**.

Nove pakete za **Debian** možete instalirati na uobičajeni način:

```
apt-get update
apt-get upgrade
```

Više informacija na:
http://www.debian.org/security/2013/dsa-2621 [1]

CARNet, Grupa za izradu paketa
paketi@carnet.hr
http://paketi.carnet.hr/ [2]

pet, 2013-02-15 09:18 - Uredništvo**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1208

Links
[1] http://www.debian.org/security/2013/dsa-2621
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr/taxonomy/term/14
[4] https://sysportal.carnet.hr/taxonomy/term/30