Sigurnosni nedostatak programskog paketa OpenSSL

Pronađen je sigurnosni propust u načinu na koji **openssl** upravlja eksplicitno zadanim inicijalizacijskim vektorima za **CBC** način enkripcije, a koji se koriste u **TLS 1.1**, **1.2** i **DTLS**-u. Krivi izračuni vode do cjelobrojnog podljeva i neispravnog pristupa memoriji, što naposljetku uzrokuje rušenje aplikacije (**DoS**) koja koristi **openssl** paket.

Ova ranjivost ima oznake: **CVE-2012-2333** i **DSA-2475-1**.

Ranjivost je ispravljena u paketu openssl verzije **0.9.8o-4squeeze13** 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/2012/dsa-2475 [1]

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

pon, 2012-05-21 09:21 - Toni Pralas**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1012

Links
[1] http://www.debian.org/security/2012/dsa-2475
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr./taxonomy/term/14
[4] https://sysportal.carnet.hr./taxonomy/term/30