Sigurnosni nedostatak unutar programskog paketa OpenSSL

 U radu programskog paketa **OpenSSL** uočen je novi sigurnosni nedostatak. Radi se o paketu koji implementira sigurnosne protokole **SSL** (eng. *Secure Sockets Layer*) i **TLS** (eng. *Transport Layer Security*) te uz to pruža i osnovnu kriptografsku podrsku.

Ranjivost je posljedica pogrešne obrade koda u dodatku za **TLS** poslužitelj te se mogla iskoristiti za rušenje aplikacije ili izvodjenje proizvoljnog programskog koda koristeci preljev memorijskog međuspremnika. Ranjivi su oni poslužitelji koji koriste višelinijsku obradu podataka (eng. *multi-thread*) i internu pričuvnu memoriju.

Ova ranjivost ima oznake: **CVE-2010-3864** i **DSA-2125-1**.

Ranjivost je ispravljena u paketu **openssl** verzije **0.9.8g-15+lenny9** za **Debian lenny**.

Nove pakete za Debian možete instalirati na uobičajeni način:

```
apt-get update

apt-get upgrade
```

Ako želite instalirati samo ove pakete:

```
apt-get update

apt-get -y install openssl libssl0.9.8
```

Više informacija na:
http://www.debian.org/security/2010/dsa-2125 [1]

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

uto, 2010-11-23 12:14 - Toni Pralas**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/793

Links
[1] http://www.debian.org/security/2010/dsa-2125
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr/taxonomy/term/14
[4] https://sysportal.carnet.hr/taxonomy/term/30