Sigurnosni nedostatak unutar programskog paketa OpenSSL

U besplatnoj implementaciji **SSL** (eng. *Secure Sockets Layer*) protokola, paketu **OpenSSL**, otkriveno je više ranjivosti. Riječ je o različitim **DoS** (eng. *Denial of Service*) ranjivostima u implementaciji **DTLS** (eng. *Datagram Transport Layer Security*) protokola te o slabostima MD2 algoritma za izračunavanje sažetaka poruke (eng. *hash*).

Zbog ranjivosti spomenutog algoritma onemogućeno je njegovo korištenje u novijim inačicama alata. Osim toga, otklonjeni su svi uočeni **DoS** problemi.

Ove ranjivost ima oznake **CVE-2009-2409** i **DSA-1888-1**.

Ranjivost je ispravljena u paketu **openssl** verzije **0.9.8c-4etch9** za **Debian etch** te verzije **0.9.8g-15+lenny5** 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/2009/dsa-1888 [1]

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

pet, 2009-09-18 15:01 - Toni Pralas**Vijesti:** Sigurnosni propusti [3]
Vote: 0

No votes yet

Links
[1] http://www.debian.org/security/2009/dsa-1888
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr./taxonomy/term/14