

## Sigurnosni nedostatak unutar programskog paketa OpenSSL

Kod paketa **OpenSSL**, koji implementira **SSL v2/3** (eng. *Secure Socket Layer*) i **TLS v1** protokole, otkriven je sigurnosni nedostatak. Uzrok sigurnosne ranjivosti je pogreška u funkciji "**ASN1\_STRING\_print\_ex**", a očituje se prilikom rukovanja s "**BMPString**" i "**UniversalString**" nizovima. Zlouporabom opisnog propusta napadač može izvesti napad uskraćivanja usluga (eng. *Denial of Service*).

Ove ranjivost ima oznake **CVE-2009-0590** i **DSA-1763-1**.

Propust je ispravljen u paketu **openssl** verzije **0.9.8c-4etch5** za **Debian etch** te verzije **0.9.8g-15+lenny1** 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-1763> [1]

CARNet, Grupa za izradu paketa

[paketi@carnet.hr](mailto:paketi@carnet.hr)

<http://paketi.carnet.hr/> [2]

uto, 2009-04-07 22:00 - Toni Pralas **Vijesti: Sigurnosni propusti** [3]

**Vote:** 0

No votes yet

**Source URL:** <https://sysportal.carnet.hr/node/554>

### Links

[1] <http://www.debian.org/security/2009/dsa-1763>

[2] <http://paketi.carnet.hr/>

[3] <https://sysportal.carnet.hr/taxonomy/term/14>