

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 podršku. Nedostatak je vezan uz pogrešku koja se javlja prilikom korištenja biblioteke **zlib**.

Spomenuti propust udaljenim zlonamjernim korisnicima omogućuje izvodjenje napada uskraćivanjem usluga (eng. *Denial of Service*).

Ova ranjivost ima oznake **CVE-2009-4355** i **DSA-1970-1**.

Ranjivost je ispravljena u paketu **openssl** verzije **0.9.8g-15+lenny6** za **Debian lenny**. Paket za **Debian etch** nije ranjiv.

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-1970> [1]

CARNet, Grupa za izradu paketa

paketi@carnet.hr

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

pet, 2010-01-15 14:53 - Toni Pralas **Vijesti:** [Sigurnosni propusti](#) [3]

Kategorije: [Sigurnost](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/697>

Links

[1] <http://www.debian.org/security/2010/dsa-1970>

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

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

[4] <https://sysportal.carnet.hr/taxonomy/term/30>

