

Sigurnosni nedostatak unutar programskog paketa OpenSSL



Otkriven je sigurnosni nedostatak u radu programskog paketa **OpenSSL**. Radi se o paketu koji implementira sigurnosne protokole **SSL** (eng. **Secure Sockets Layer**) i **TLS** (eng. **Transport Layer Security**).

Navedeni je nedostatak posljedica neodgovarajuće provjere povratnih vrijednosti u funkciji "**EVP_VerifyFinal**". Udaljeni, zlonamjerni korisnik može iskoristiti navedenu ranjivost za zaobilaženje pojedinih sigurnosnih provjera.

Ove ranjivost ima oznake **CVE-2008-5077** i **DSA-1701-1**.

Propust je ispravljen u paketu **openssl** verzije **0.9.8c-4etch4** za **Debian etch**.

Novo pakete za Debian možete instalirati na uobičajeni način:

```
apt-get update
```

```
apt-get upgrade
```

Ako želite instalirati samo openssl pakete:

```
apt-get update
```

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

Više informacija na:

<http://www.debian.org/security/2009/dsa-1701> [1]

CARNet, Grupa za izradu paketa

paketi@carnet.hr

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

sri, 2009-01-14 11:08 - Toni Pralas **Vijesti:** [Sigurnosni propusti](#) [3]

Kategorije: [Sigurnost](#) [4]

Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/498?page=0>

Links

- [1] <http://www.debian.org/security/2009/dsa-1701>
- [2] <http://paketi.carnet.hr/>
- [3] <https://sysportal.carnet.hr/taxonomy/term/14>
- [4] <https://sysportal.carnet.hr/taxonomy/term/30>