

Sigurnosni nedostatak OpenSSL programskog paketa



Unutar OpenSSL programskog paketa primjećen je sigurnosni propust. OpenSSL je implementacija SSL (*Secure Sockets Layer*) i TLS (*Transport Layer Security*) protokola te raznih kriptografskih algoritama.

Spomenuti propust odnosi se na "SSL_get_shared_ciphers()" funkciju koja, zbog pogreške u izvedbi jedne programske petlje, zlonamjernom napadaču omogućava rušenje osjetljive aplikacije, ali i pokretanje izvođenja proizvoljnog programskog koda s ovlastima korisnika koji je pokrenuo aplikaciju.

Spomenuta ranjivost ima oznake CVE-2007-5135 i DSA 1379-1. Propust je ispravljen u paketu openssl verzije 0.9.7e-3sarge5 za Debian Sarge (CARNet Debian 2.1).

Novi paketi za Debian mogu se instalirati na uobičajeni način:

```
apt-get update  
apt-get upgrade
```

tj. prilikom instalacije samo openssl paketa:

```
apt-get update  
apt-get -y install openssl libssl0.9.7
```

Više informacija nalazi se na:

<http://www.debian.org/security/2007/dsa-1379>

pet, 2007-10-05 08:38 - Uredništvo **Vijesti:** [Sigurnosni propusti](#) [1]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/300>

Links

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