

## Sigurnosni nedostaci OpenSSL-a



Ispravljene su sigurnosni propusti programskog paketa **openssl** na operacijskom sustavu **Debian**. Propusti proizlaze iz nepravilne implementacije **DTLS**, **SSL 3.0** i **Server Gated Cryptography (SGC)**, dvostrukog oslobađanja memorije kada je uključen **X509\_V\_FLAG\_POLICY\_CHECK**, te neispravne implementacije **P-256** i **P-384** operacija **NIST** eliptičkih krivulja na 32-bitnim sustavima. Udaljeni napadači propuste mogu iskoristiti za povrat informacija u *plaintext* formatu, pribavljanje osjetljivih informacija te uskraćivanje usluge.

Ove ranjivosti imaju oznake: **CVE-2011-4108**, **CVE-2011-4109**, **CVE-2011-4354**, **CVE-2011-4576**, **CVE-2011-4619** i **DSA-2390-1**.

Ranjivosti su ispravljene u paketu openssl verzije **0.9.8g-15+lenny15** za **Debian lenny**.

Novo pakete za **Debian** možete instalirati na uobičajeni način:

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

Više informacija na:

<http://www.debian.org/security/2012/dsa-2390> [1]

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

sri, 2012-01-18 11:32 - Toni Pralas **Vijesti: Sigurnosni propusti** [3]

**Kuharice:** [Linux](#) [4]

**Vote:** 0

No votes yet

**Source URL:** <https://sysportal.carnet.hr./node/917>

### Links

[1] <http://www.debian.org/security/2012/dsa-2390>

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

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

[4] <https://sysportal.carnet.hr./taxonomy/term/17>