

Sigurnosni nedostaci paketa OpenSSL



Ispravljene su tri ranjivosti u radu programskog paketa **OpenSSL** na operacijskom sustavu **Debian**. Ranjivosti su uzrokovane pogreskom u **CMS** i **PKCS #7** dekriptijskom kodu, dereferenciranjem **NULL** pokazivača u funkciji "**mime_param_cmp()**" (**crypto/asn1/asn_mime.c**) prilikom parsiranja određenih **MIME** zaglavlja i nepravilnom provjerom graničnih vrijednosti kod obrade **DER** podataka putem **BIO** ili **FILE** funkcija.

Napadaču je omogućeno dekriptiranje podataka putem "**Million Message Attack**" (**MMA**) napada, izvoenje **DoS** napada i pokretanje proizvoljnog programskog koda.

Ove ranjivosti imaju oznake: **CVE-2012-0884**, **CVE-2012-1165**, **CVE-2012-2110** i **DSA-2454-1**.

Ranjivost je ispravljena u paketu openssl verzije **0.9.8o-4squeeze11** za **Debian squeeze**.

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

```
apt-get update
```

```
apt-get upgrade
```

Više informacija na:

<http://www.debian.org/security/2012/dsa-2454> [1]

CARNet, Grupa za izradu paketa

paketi@carnet.hr

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

pon, 2012-04-23 09:47 - Toni Pralas **Vijesti:** [Sigurnosni propusti](#) [3]

Kategorije: [Sigurnost](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/992>

Links

[1] <http://www.debian.org/security/2012/dsa-2454>

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

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

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

