Sigurnosni nedostatak unutar DNS poslužitelja BIND 9

Kod programskog paketa **BIND 9** (eng. *Berkeley Internet Name Domain*) otkriven je sigurnosni problem. Radi se o paketu koji implementira **DNS** (eng. ***Domain Name System***) protokol na operacijskim sustavima ***Unix/Linux***.

Sigurnosna je ranjivost posljedica nepravilnosti u radu funkcije "***OpenSSL DSA_verify***". Zlouporaba napadaču omogućuje zaobilaženje ispravne provjere niza certifikata podmetanjem posebno oblikovanih SSL/TLS potpisa.

Ova ranjivost ima oznake: **CVE-2009-0025** i **DSA-1703-1**.

Propust je ispravljen u paketu **bind9** verzije **9.3.4-2etch4** za **Debian etch**.

Novi paket **bind9** za **Debian etch** možete instalirati na uobičajeni način:

```
apt-get update

apt-get upgrade
```

Ako želite instalirati samo **bind9** paket:

```
apt-get update

apt-get -y install bind9
```

Više o tome na:
http://www.debian.org/security/2009/dsa-1703 [1]

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

sri, 2009-01-14 10:59 - Toni Pralas**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/496

Links

[1] http://www.debian.org/security/2009/dsa-1703
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr./taxonomy/term/14
[4] https://sysportal.carnet.hr./taxonomy/term/30