Sigurnosni nedostaci unutar DNS posluzitelja BIND9

U programskom paketu **BIND**, koji sadrži implementaciju protokola **DNS** (eng. **Domain Name System**), otkrivene su tri ranjivosti. Propusti su vezani uz neodgovarajuću obradu poruka koje poslužitelj prima od udaljenih sustava.

Slanjem posebno oblikovanih poruka BIND poslužitelju, moguće je neovlašteno izmijeniti sadrzaj DNS priručne memorije. Posljedica uspješnog
napada je mogućnost preusmjeravanja zahtjeva korisnika na zloćudna odredišta.

Ove ranjivosti imaju oznake: CVE-2010-0097, CVE-2010-0290, CVE-2010-0382 i DSA-2054-1.

Propusti su ispravljeni u paketu bind9 verzije 1:9.6.ESV.R1+dfsg-0+lenny1 za Debian lenny.

Nove pakete za Debian možete instalirati na uobičajeni način:

```
apt-get update

apt-get upgrade
```

Ako želite instalirati samo paket bind9:

```
apt-get update

apt-get -y install bind9
```

Više o tome možete naći na:
http://www.debian.org/security/2010/dsa-2054 [1]

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

čet, 2010-06-10 09:14 - Toni Pralas**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/749

Links

[1] http://www.debian.org/security/2010/dsa-2054
[2] http://paketi.carnet.hr/
[3] https://sysportal.carnet.hr/taxonomy/term/14
[4] https://sysportal.carnet.hr/taxonomy/term/30