

Sigurnosni nedostaci unutar programskog paketa OpenSSH



Prilikom rukovanja s programskim paketom **OpenSSH** otkrivene su dvije sigurnosne ranjivosti. Radi se o besplatnoj implementaciji **SSH** (eng. *Secure Shell*) protokola koji ostvaruje sigurnu komunikaciju putem računalne mreže.

Jedan od propusta vezan je uz nesigurno rukovanje signalima, dok se drugi javlja ukoliko je aplikacija postavljena tako da prihvaća **GSSAPI** autentikaciju.

Opisani propusti omogućuju stvaranje **DoS** (eng. *Denial of Service*) uvjeta i pokretanje proizvoljnog programskog koda na ranjivom računalu. Ove ranjivosti imaju oznake **CVE-2008-4109** i **DSA-1638-1**. Propust je ispravljen u paketu **openssh** verzije **4.3p2-9etch3** za **Debian Etch**.

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

- *apt-get update*
- *apt-get upgrade*

Ako želite instalirati samo **OpenSSH** pakete:

- *apt-get update*
- *apt-get -y install openssh-client openssh-server*

Više informacija imate na:

<http://www.debian.org/security/2008/dsa-1638> [1]

CARNet

Grupa za izradu paketa

paketi@carnet.hr

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

sri, 2008-09-24 09:28 - Toni Pralas **Vijesti: Sigurnosni propusti** [3]

Kategorije: [Sigurnost](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/429>

Links

- [1] <https://webmail.carnet.hr/horde/util/go.php?url=http%3A%2F%2Fwww.debian.org%2Fsecurity%2F2008%2Fdsa-1638&Horde=06ae15f6da4435781f9520f8aa4591e3>
- [2] <http://paketi.carnet.hr/>
- [3] <https://sysportal.carnet.hr/taxonomy/term/14>
- [4] <https://sysportal.carnet.hr/taxonomy/term/30>