Sigurnosni nedostatak unutar programskog paketa GnuPG

Kod GnuPG programskog paketa otkriven je sigurnosni nedostatak. GnuPG (eng. GNU Privacy Guard) je implementacija OpenPGP standarda i koristi se za kriptiranje i digitalno potpisivanje datoteka i poruka.

Nova inačica ovog paketa je izdana zbog izmjena startnih postavki kojima se ne dozvoljavaju višestruki elementi običnog teksta unutar iste poruke. Propust omogućava zlonamjernom napadaču dodavanje poruke ispred digitalno potpisane poruke, čime se korisnik dovodi u zabludu da je cijela poruka digitalno potpisana i poslana od originalnog posiljatelja.

Ranjivosti imaju oznake: CVE-2007-1263 i DSA 1266-1. Propusti su ispravljeni u paketu gnupg verzije 1.4.1-1.sarge7 za Debian Sarge.

Novi paket može se instalirati na uobičajeni način:

apt-get update
apt-get upgrade

tj. u slučaju instalacije samo ovog paketa:

apt-get update
apt-get -y install gnupg.

Više informacija nalazi se na:
http://www.debian.org/security/2007/dsa-1266

pon, 2007-03-19 09:21 - Uredništvo**Vijesti:** Sigurnosni propusti [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/125

Links
[1] https://sysportal.carnet.hr/taxonomy/term/14