

Sigurnosni nedostaci unutar PHP5



U radu programskog paketa **PHP5** otkriveno je više sigurnosnih nedostataka. Riječ je o interpreteru istoimenog, objektno-orijentiranog skriptnog jezika. Bitniji su propusti uzrokovani neodgovarajućim postavljanjem varijabli "**page_uid**" i "**page_gid**" te nepravilnostima u funkcijama "**ZipArchive::extractTo()**" i "**JSON_parser()**".

Napadaču omogućuju prepisivanje proizvoljnih datoteka, povećanje ovlasti, izvođenje **DoS** napada i dr. Za detaljniji uvid u sve propuste savjetuje se čitanje izvorne preporuke.

Propusti imaju oznake: **CVE-2008-2107**, **CVE-2008-2108**, **CVE-2008-5557**, **CVE-2008-5624**, **CVE-2008-5658**, **CVE-2008-5814**, **CVE-2009-0754**, **CVE-2009-1271** i **DSA-1789-1**.

Propusti su ispravljeni u paketima **php5-*** verzije **5.2.0+dfsg-8+etch15** za **Debian Etch**, te verzije **5.2.6.dfsg.1-1+lenny3** za **Debian Lenny**.

Više informacija na:

<http://lists.debian.org/debian-security-announce/2009/msg00100.html> [1]

CARNet, Grupa za izradu paketa

paketi@carnet.hr

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

sri, 2009-05-06 09:00 - Toni Pralas **Vijesti:** [Sigurnosni propusti](#) [3]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/573>

Links

[1] <http://lists.debian.org/debian-security-announce/2009/msg00100.html>

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

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