

Novi nedostaci unutar PHP4 i PHP5 programskih paketa



Unutar PHP4 i PHP5 programskog paketa uočeno je nekoliko sigurnosnih nedostataka. PHP je interpreter istoimenog skriptnog jezika namijenjenog izradi dinamičkih web stranica. Svi novootkriveni propusti za posljedicu mogu imati izvršavanje proizvoljnog programskog koda na udaljenom računalu.

Kod PHP5 paketa prepisivanje spremnika (*buffer overflow*) kod zip i xmlrpc ekstenzija može dovesti do izvršavanja proizvoljnog koda. Više informacija o spomenutim nedostacima pod oznakama CVE-2007-1399 i CVE-2007-1864 nalazi se [ovdje](#) [1].

Osim propusta prilikom prepisivanja spremnika kod xmlrpc ekstenzije, unutar PHP4 programskog paketa ranjivost se javlja kod prepisivanja cjelobrojne varijable prilikom alokacije memorije te zbog nedostataka kod interpretacije HTTP protokola. Detaljnije o propustima pod oznakama CVE-2006-4486 i CVE-2006-0207 nalazi se [ovdje](#) [2].

pon, 2007-07-09 14:54 - Uredništvo **Vijesti:** [Linux](#) [3]
[Sigurnost](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/245>

Links

- [1] <http://www.debian.org/security/2007/dsa-1330>
- [2] <http://www.debian.org/security/2007/dsa-1331>
- [3] <https://sysportal.carnet.hr/taxonomy/term/11>
- [4] <https://sysportal.carnet.hr/taxonomy/term/13>