

Sigurnosni nedostaci unutar PHP 4



Unutar PHP 4 prevodioca otkriveni su višestruki sigurnosni propusti. Nedostaci nastaju zbog cjelobrojnog prepisivanja unutar 'str_replace()' funkcije, zbog podljeva spremnika kod 'sapi_header_op()' funkcije, unutar 'wddx' dodatka, zbog nesigurnog rukovanja znakovnim nizovima u 'odbc_result_all()' funkciji, zbog nesigurnog rukovanja 'super-global' varijablama i beskonacne petlje unutar 'zend_hash_init()' funkcije.

Napadač može iskoristiti navedene ranjivosti za pokretanje proizvoljnog programskog koda, izvođenje napada uskraćivanjem usluga ili neovlašten pristup potencijalno osjetljivim podacima.

Propusti imaju oznake CVE-2007-0906, CVE-2007-0907, CVE-2006-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-0988 i DSA 1264-1. Propusti su ispravljani u Debianovim paketima verzije 4.3.10-19 za Debian Sarge.

Novi paketi za Debian mogu se instalirati na uobičajeni način:

```
apt-get update  
apt-get upgrade
```

tj. u slučaju instalacije isključivo ovog paketa:

```
apt-get update  
apt-get -y install php4
```

Više informacija nalazi se na adresi:

<http://www.debian.org/security/2007/dsa-1264> [1]

pet, 2007-03-16 23:50 - Uredništvo **Vijesti:** [Sigurnosni propusti](#) [2]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/124>

Links

[1] <http://www.debian.org/security/2007/dsa-1264>

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