Nesigurna konfiguracija Apache2 servera

Na Debianu instalacija paketa Apache2 smješta skripte, koje se isporučuju kao primjeri, u direktorij /usr/share/doc, koji je u konfiguraciji mapiran na /doc. Ukoliko imate instalirane module mod_php ili mod_rivet, napadač može pokrenuti te skripte. Iako je mogućnost napada ograničena samo na lokalne korisnike, navode se dva primjera kako se ranjivost može iskoristiti i za udaljeni napad.

- ako web server prosljeđuje upit pozadinskom apache web serveru na localhost adresi
- ako se računalo na kojem je pokrenut apache koristi i za surfanje

Kako su na mnogim ustanovama web serveri ujedno i računala na kojima studenti i zaposleni imaju otvorene korisničke račune, netko bi od korisnika mogao iskoristiti ovu ranjivost.

U trenutno stabilnoj distribuciji, Squeeze, ovaj je problem uklonjen u paketu 2.2.16-6+squeeze7.

Ako ste još na Lennyju, tada iz konfiguracije u /etc/apache2/sites-available/* uklonite direktive

```
Alias /doc "/usr/share/doc"
```

i cijeli blok

```
<Directory "/usr/share/doc/">
```

pon, 2012-04-16 10:00 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/982

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