

## How to disable Debian GNU / Linux (Squeeze) Apache 2 version reporting to improve security - Hide Apache server version

Author : admin

Debian GNU / Linux's Apache default behavior is to *report Apache server name, version and Linux distribution version and codename*.

This is shown as a minor security leak in many Security Scanner (audit) software like Nessus. It reveals a vital information which could help malicious attacker later to use exploit if the version number in question is vulnerable.

The quickest way to check, either Apache versioning and distro info is disabled is with *telnet*:

```
hipo@noah:~/Desktop$ telnet pc-freak.net 80
Trying 83.228.93.76...
Connected to pc-freak.net.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
Connection closed by foreign host.
hipo@noah:~/Desktop$ telnet pc-freak.net 80
Trying 83.228.93.76...
Connected to pc-freak.net.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
Date: Fri, 05 Oct 2012 10:48:36 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze14
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

Disabling this *Distro version codename and version number reporting* on Debian is done by changing in file **/etc/apache2/conf.d/security** directives:

```
ServerTokens OS
ServerSignature On
```

to

ServerSignature Off  
ServerTokens ProductOnly

Here important note to make is if you try adding:

**ServerSignature Off** and **ServerTokens Prod** straight in Debian general config */etc/apache2/apache2.conf*, but did not change the settings set for the vars through */etc/apache2/conf.d/security*; settings from */etc/apache2/conf.d/security* will overwrite *ServerSignature* / *ServerTokens* settings set in ***/etc/apache2/apache2.conf***

I tried this myself (forgetting about */etc/apache2/conf.d/security*) and adding both variables straight in *apache2.conf*. After Apache restart Apache version number and type of distribution continued be returned by the WebServer.

I thought something specific changed in *Debian Squeeze - Apache/2.2.16* so this two variables are probably not working so I did a quick research online seeing other people complaining also *unable to disable Apache ver and Linux distro version* and looking for a reason why. Well anyways if you happen to also ponder, why *ServerSignature Off* and *ServerTokens ProductOnly* does not take effect keep in mind it is due to overwritten settings via */etc/apache2/conf.d/security*, changing the values there and restarting Apache and you're done :)

To make sure 100% Apache is no longer returning exact version number and host installed distro type, use *telnet* again:

```
hipo@noah:~/Desktop$ telnet pc-freak.net 80
Trying 83.228.93.76...
Connected to pc-freak.net.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
Connection closed by foreign host.
```