

ModSSL – Knoppix 3.3

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-03/0002.html>

From: Bernard, Cyrille (*Cyrille.Bernard_at_BEIJAFLORE.com*)

Date: 03/16/04

Date: Tue, 16 Mar 2004 15:45:11 +0100

To: <focus-linux@securityfocus.com>

hi everyone.

it's not really a matter of security here. But i've some trouble with apache 1.3.29, mod_ssl/2.8.14 and OpenSSL/0.9.7b

I use the knoppix 3.3 hd installation. It comes with all stuff.
I create some server key & crt. And set up things in httpd.conf

the main lines are :

Port 80

User www-data

Group www-data

ServerAdmin root@shuttlex

ServerName shuttlex

DocumentRoot /var/www

[...]

Listen 80

Listen 443

NameVirtualHost 192.168.1.1:443

NameVirtualHost 192.168.1.1:80

<VirtualHost 192.168.1.1>

SSLEngine Off

</VirtualHost>

<VirtualHost 192.168.1.1:443>

CustomLog logs/ssl_request_log "%t %h % {SSL_PROTOCOL}x % {SSL_CIPHER}x \"%r\" %b"

TransferLog logs/ssl_access_log

SSLEngine On

SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile /etc/apache/conf/ssl.crt/server.crt

SSLCertificateKeyFile /etc/apache/conf/ssl.key/server.key

SecurityFocus Linux: ModSSL – Knoppix 3.3

```
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown downgrade-1.0 force-response-1.0
<Directory "/usr/local/apache/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
<Files ~ "\.(cgi|shtml|phtml|php3?)|php|inc)$">
    SSLOptions +StdEnvVars
</Files>

</VirtualHost>
```

The problem is :

- i can do http and https request from the local server (browser konqueror)
- i can do http request but NOT https request with a remote client (browser IE)
- i can do ssh remote and telnet request on port 443 from remote
- i can do https request on some other ssl server (lan or internet)

What i've done to test things :

```
netstat -na looks ok
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
```

let says my local ip is 192.168.1.1 (apache server) and my remote is 192.168.1.2 (client)
when i telnet 443 the server from the client
tcp 0 0 192.168.1.1:443 192.168.1.2:2396 ESTABLISHED
when i use the browser with https, nothing happend

there's no FW/ACL between client/server. I've try a direct connection too with a crossover cable.
i've try some change with httpd.conf (not to use virtual host, but it's the same).

- I dont have any trouble with other linux/apachesslinstallation
- I dont see anything significative in the logs files

So, is it me or is there a bug out there ?

Sum up :

from REMOTE : ssh ok, http ok, https NOK.
from LOCAL http ok, https ok

thx for help.

cdt,

Cyrille (FRANCE)