

# Faile Poodle

Des clients peuvent être attaqués via le protocole SSL V3 <sup>1)</sup>. L'authentification (donc l'envoi du mot de passe ou du numéro de la carte bleue) se fait avant le chiffrement <sup>2)</sup>.

En attendant la mise à jour des logiciels, il faut forcer l'utilisation de TLS <sup>3)</sup>, plus récent que SSL v3 <sup>4)</sup>

## Interdire le SSL V3 dans Firefox

### about:config

Pour modifier la configuration de Firefox, taper “about:config” dans la barre d'URL.



### security.tls.version.min=1

Rechercher ensuite le paramètre security.tls.version.min.



Double-cliquer sur la ligne pour modifier la valeur..



## Chromium

Il faut ajouter **-ssl-version-min=tlsl** dans toutes les lignes qui commencent par “Exec=” dans le fichier de configuration (/usr/share/applications/chromium-browser.desktop sur ubuntu) <sup>5)</sup>

[/usr/share/applications/chromium-browser.desktop](#)

```
Exec=chromium-browser --ssl-version-min=tlsl %U
Exec=chromium-browser --ssl-version-min=tlsl
Exec=chromium-browser --incognito --ssl-version-min=tlsl
Exec=chromium-browser --temp-profile --ssl-version-min=tlsl
```

## Pour tester son site préféré

Tapez la commande suivante en ligne de commande, en remplaçant labs.core-cloud.net par l'URL du site à tester :

```
openssl s_client -connect labs.core-cloud.net:443 -ssl3
```

Si vous obtenez une réponse du type "handshake failure", c'est bon :

```
140333026707104:error:14094410:SSL routines:SSL3_READ_BYTES:ssl3 alert  
handshake failure:s3_pkt.c:1260:SSL alert number 40  
140333026707104:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake  
failure:s3_pkt.c:596:
```

Sinon, c'est que le serveur n'a pas été mis à jour :

```
depth=2 C = US, ST = UT, L = Salt Lake City, O = The USERTRUST Network, OU =  
http://www.usertrust.com, CN = UTN-USERFirst-Hardware
```

[nouveau, securite](#)

1)

Pour tout savoir, lire la synthèse de Stéphane Bortzmeyer <http://seenthis.net/messages/302666>

2)

Documentation technique qui explique tout : <https://www.imperialviolet.org/2014/10/14/poodle.html>

3)

1999 pour la version TLS 1.0 <https://tools.ietf.org/html/rfc2246>

4)

1996 : <https://tools.ietf.org/html/rfc6101>

5)

<http://askubuntu.com/questions/537196/how-do-i-patch-workaround-ssl3-poodle-vulnerability-cve-2014-3566>

From:

<https://amic.limsi.fr/> - **Administration des moyens informatiques communs.**

Permanent link:

<https://amic.limsi.fr/doku.php?id=poodle&rev=1413379047>

Last update: **2014/10/15 15:17**

