Faille Poodle

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

En attendant la mise à jour des logiciels, il faut forcer l'utilisation de TLS 1.0 (au minimum) [3)], plus récent que SSL v3 [4)]

Mise à jour des postes utilisateurs

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=tls1** dans toutes les lignes qui commencent par “Exec=” dans le fichier de configuration (/usr/share/applications/chromium-browser.desktop sur ubuntu) [5)]

/usr/share/applications/chromium-browser.desktop

```
Exec=chromium-browser --ssl-version-min=tls1 %U
Exec=chromium-browser --ssl-version-min=tls1
Exec=chromium-browser --incognito --ssl-version-min=tls1
Exec=chromium-browser --temp-profile --ssl-version-min=tls1
```

Mise à jour des serveurs

Les administrateurs système doivent aussi mettre leurs serveurs à jour... Par exemple pour Apache, il faut rechercher le paramètre SSLProtocol et le modifier comme suit [6)]

/etc/apache2/mods-available/ssl.conf

```
SSLProtocol all -SSLv3
```

Pour tester un serveur web

Tapez la ligne de commande suivante dans un terminal (unix, mac), 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:sslv3 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) , 6) http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566