Faille Poodle

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

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) [2]

/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
```

nouveau, securite

1)
Voir : https://www.imperialviolet.org/2014/10/14/poodle.html

2)
http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-20

14-3566