



Forum: Généralités

Topic: BULLETIN D'ALERTE DU CERT-FR DU 14 octobre 2014: Vulnérabilité dans SSLv3

Subject: BULLETIN D'ALERTE DU CERT-FR DU 14 octobre 2014: Vulnérabilité dans SSLv3

Publié par: ribotb

Contribution le : 16/10/2014 14:00:22

Une vulnérabilité a été découverte dans la version 3 du protocole SSL permettant de sécuriser les connexions entre clients et serveurs. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données, par exemple de récupérer un cookie de session HTTPS.

Contournement provisoire

Il est possible de configurer les navigateurs afin de les empêcher d'utiliser cette version du protocole :

- **pour Internet Explorer**, aller dans les "**options internet**" puis dans l'onglet "**Avancé**", dans la liste déroulante, décocher la case "**SSL 3.0**" ;
- **pour Firefox** (fonctionne aussi **pour Thunderbird**), dans la barre d'adresse, taper "**about:config**" puis rechercher "**security.tls.version.min**" et changer sa valeur à **1** ;

<http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-007/CERTFR-2014-ALE-007.html>