Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 15 octobre 2014
N° CERTFR-2014-ALE-007

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans SSLv3

Gestion du document

Référence	CERTFR-2014-ALE-007
Titre	Vulnérabilité dans SSLv3
Date de la première version	15 octobre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité du 14 octobre 2014
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

– atteinte à la confidentialité des données.

2 - Systèmes affectés

– Toutes les implémentations du protocole SSLv3 ;
– Navigateurs Web employant SSLv3, dont Internet Explorer, Firefox et Chrome.

3 - Résumé

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.

4 - Solution

L'exploitation de la vulnérabilité est basée sur la négociation protocolaire entre le client et le serveur. Le client force le serveur à utiliser SSLv3 qui est une ancienne version du protocole SSL/TLS. L'attaquant sera en mesure de déchiffrer une partie du trafic réseau vers des sites sécurisés et de récupérer des cookies de session HTTPS.

Le CERTFR recommande la désactivation du support du protocole SSLv3 au sein de tout logiciel l'implémentant.

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 ;

Pour les applications basées sur l'API Cryptographique de Windows (CAPI), il est possible de modifier la clé de registre suivante :

```
 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 3.0\Client] "Enabled"=dword:00000000
```

5 - Documentation

- Bulletin de sécurité du 14 octobre 2014 d'OpenSSL
  https://www.openssl.org/ bodo/ssl-poodle.pdf
- Référence CVE CVE-2014-3566
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

Gestion détaillée du document

15 octobre 2014 version initiale.