

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation malveillante d'une fonctionnalité du protocole SSL

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-005>

Gestion du document

Référence	CERTA-2011-ALE-005
Titre	Exploitation malveillante d'une fonctionnalité du protocole SSL afin de provoquer un déni de service
Date de la première version	27 octobre 2011
Date de la dernière version	–
Source(s)	
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

Déni de service à distance.

2 Systèmes affectés

Toutes les implémentations du protocole SSL/TLS sont potentiellement vulnérables.

3 Résumé

Le CERTA constate un intérêt renouvelé pour l'exploitation malveillante de la fonctionnalité de renégociation de clés de session du protocole SSL/TLS afin de provoquer un déni de service.

4 Description

Plusieurs articles et des outils récemment publiés sur l'Internet mettent en lumière certaines fonctionnalités du protocole SSL/TLS. En effet, le protocole SSL requiert des traitements significativement plus coûteux pour le serveur que le client lors de l'établissement d'une session ou lors de la renégociation de clés de session. Cette forte asymétrie des traitements entre le client et le serveur permet à un ou plusieurs clients d'épuiser les ressources

serveur et de réaliser un déni de service. Les publications récentes détaillent ces aspects et proposent des outils, très simples d'utilisation, mettant en pratique cette attaque.

Toutes les applications reposant sur l'utilisation d'un canal SSL/TLS sont potentiellement vulnérables (HTTPS, POP3, IMAPS, LDAPS, ...).

La plus efficace de ces attaques consiste à utiliser une seule connexion TCP pour réaliser de nombreuses renégociations des clés de session SSL/TLS.

Une variante de cette attaque, plus facilement détectable, consiste pour le client à multiplier les connexions TCP pour établir un grand nombre de sessions SSL/TLS. Cette variante sera privilégiée par l'attaquant lorsque la renégociation de clés de session initiée par le client est désactivée sur le serveur.

5 Mesures de contournement

S'agissant d'une fonctionnalité du protocole SSL/TLS, aucun correctif n'est à attendre de la part des éditeurs d'implémentation du protocole SSL/TLS.

Néanmoins, un certain nombre de vérifications et/ou précautions s'imposent pour prévenir un déni de service sur des applications critiques reposant sur le protocole SSL/TLS.

5.1 Désactivation de la fonctionnalité de renégociation de clés de session initiée par le client

La fonctionnalité de renégociation des clés de session a déjà donné lieu à la publication de l'avis CERTA-2009-AVI-482. Lors du traitement de cette vulnérabilité, les différents éditeurs d'implémentation du protocole SSL/TLS ont proposé des mises à jour refusant par défaut les demandes de renégociation de clés de session initiées par le client.

Pour l'implémentation OpenSSL, la version OpenSSL 0.9.8l désactive la renégociation de clé initiée par le client. Les versions 0.9.8m et supérieures réactivent cette fonctionnalité. Il revient alors à l'administrateur de s'assurer que les applications proposant un canal chiffré avec OpenSSL sont configurées pour refuser les demandes de renégociation des clés de session. Par exemple, le module `mod_ssl` de Apache rejette ces demandes dans les versions récentes.

Pour l'implémentation de Microsoft Windows (Schannel), les mises à jour de `Schannel.dll` sont documentées dans l'avis de sécurité Microsoft KB977377.

Ces mises à jour désactivent par défaut la renégociation de clés de session initiée par le client. Il est important de bien noter que les vulnérabilités adressées par ces mises à jour ne sont pas liées aux exploitations malveillantes par déni de service décrites dans cette alerte.

Cette mesure permet de prévenir l'exploitation la plus efficace de cette vulnérabilité.

5.2 Surveillance et limitation des connexions TCP

L'autre technique ici utilisée est un déni de service plus classique reposant sur la multiplication des connexions au serveur et le déclenchement de traitements coûteux pour le serveur (ici l'établissement de sessions SSL/TLS).

Dans ce contexte, il convient de recourir au moyen habituels de prévention de ce risque :

- Augmentation des capacités du serveur

L'attaque reposant sur l'attrition des ressources du serveur, il peut suffire d'augmenter significativement les capacités de traitement afin de pouvoir absorber la charge de l'attaque sans impacter la charge normale de l'application.

- Limitation du nombre de connexions

L'application de mesures de limitation du nombre de connexions TCP simultanées va efficacement limiter l'accès de l'attaquant aux ressources du serveur et ainsi prévenir l'attaque.

- Utilisation de matériel spécialisé type *Hardware Security Module* (HSM)

Des matériels spécialisés type HSM permettent d'augmenter significativement le nombre de négociations SSL/TLS réalisées par unité de temps et donc la résistance aux attaques. Lorsque ces boîtiers sont utilisés, il est important de s'assurer que les protocoles acceptés par l'application côté serveur sont bien accélérés par ce matériel. En effet, si un protocole négocié entre le client et le serveur n'est pas accéléré alors la protection apportée par le dispositif n'est plus efficace.

6 Documentation

- Avis CERTA-2009-AVI-482
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-482>
- Bulletin d'actualité CERTA-2009-ACT-046
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-046>
- ChangeLog OpenSSL
<http://openssl.org/news/changelog.html>
- Avis de sécurité Microsoft: Une vulnérabilité de TLS/SSL pourrait permettre l'usurpation d'identité
<http://support.microsoft.com/kb/977377/fr>

Gestion détaillée du document

27 octobre 2011 version initiale.