

Vulnérabilités dans le composant OpenSSL intégré dans les produits SSL360

Date de découverte	28 Septembre 2006
Révision du bulletin	AK-2006-08 1.1 (10 Octobre 2006)
Gravité	Haute
Impact	Déni de Service
Niveau de compétence requis de l'attaquant	Expert
Provenance de l'attaque	Réseaux autorisés
Popularité	Haute
Versions SSL360 concernées	Toutes avant 2.0/3

Introduction

De multiples vulnérabilités ont été découvertes dans le composant OpenSSL du produit SSL360. Leur exploitation peut permettre à un attaquant de faire consommer inutilement des ressources sur l'appliance.

Description

Plusieurs erreurs d'implémentation dans le composant OpenSSL peuvent permettre à un attaquant de provoquer un Déni de service, en forgeant des certificats X.509, lors de l'établissement d'une connexion SSL.

Impact

L'attaquant peut faire consommer inutilement des ressources (CPU, mémoire), ralentissant l'exécution des autres tâches effectuées par l'appliance.

Gravité

La gravité de cette vulnérabilité a été classée **haute** pour les raisons suivantes :

- Déni de service ;
- Dans certains cas d'utilisation, exploitation possible depuis Internet.



Références

- OpenSSL Security Advisory (http://www.openssl.org/news/secadv_20060928.txt)
- CVE-2006-2937 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937>)
- CVE-2006-2940 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940>)

Versions impactées

- Version majeure 1.0 : Toutes (série non maintenue)
- Version majeure 2.0 : <= 2.0/2

Solution

La version 2.0/3 comporte un correctif pour ce problème. Si votre configuration est impactée, nous vous recommandons de mettre à jour votre système dès que possible.

Note : la série SSL360 1.0 n'est plus supportée depuis la sortie de la version 2.0/1. Si votre système utilise une de ces versions, nous vous recommandons de passer en version 2.0/3 ou ultérieure dès que possible.

Si vous rencontrez des problèmes, n'hésitez pas à contacter le support Arkoon à l'adresse suivante : <http://client.arkoon.net>

Merci de votre collaboration.

Cellule Sécurité Arkoon
security@arkoon.net

