

## Vulnérabilités dans le composant OpenSSL intégré dans les produits FAST360 et AMC

<b>Date de découverte</b>	28 Septembre 2006
<b>Révision du bulletin</b>	AK-2006-06 1.1 (10 Octobre 2006)
<b>Gravité</b>	Haute
<b>Impact</b>	Déni de Service
<b>Niveau de compétence requis de l'attaquant</b>	Expert
<b>Provenance de l'attaque</b>	Réseaux autorisés
<b>Popularité</b>	Haute
<b>Versions FAST360 concernées</b>	Toutes
<b>Versions AMC concernées</b>	Toutes

### Introduction

De multiples vulnérabilités ont été découvertes dans le composant OpenSSL des produits FAST360 et AMC. Leur exploitation peut permettre à un attaquant de faire consommer inutilement des ressources sur l'apppliance ou le serveur AMC.

### 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.

Cela nécessite que l'attaquant soit autorisé à établir des connexions SSL sur l'apppliance, par exemple par le biais d'une connexion administrative (Arkoon Manager, Arkoon Monitoring, Arkoon Reporting, akslave, akha, arkupdate).

### Impact

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

### Gravité

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

- Déni de service sur un grand nombre de composants;
- Dans certains cas d'utilisation, exploitation possible depuis Internet.



## Références

- OpenSSL Security Advisory ([http://www.openssl.org/news/secadv\\_20060928.txt](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

- FAST360 :
  - Version majeure 3.0 : <= 3.0/31
  - Version majeure 4.0 : <= 4.0/4
- AMC :
  - Version majeure 1.0 : <= 1.0/5

## Solution

Les versions FAST360 3.0/32, FAST360 4.0/5 et AMC 1.0/6 comportent un correctif pour ce problème. Nous vous recommandons de mettre à jour votre système 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](mailto:security@arkoon.net)

