

Vulnérabilités dans le composant OpenSSH intégré dans les produits SSL360

Date de découverte	27 Septembre 2006
Révision du bulletin	AK-2006-09 1.0 (6 Octobre 2006)
Gravité	Moyenne
Impact	Déni de Service
Niveau de compétence requis de l'attaquant	Expert
Provenance de l'attaque	Réseaux autorisés
Popularité	Haute
Versions SSL360 concernées	2.0/1 et 2.0/2

Introduction

De multiples vulnérabilités ont été découvertes dans le composant OpenSSH du produit SSL360. Leur exploitation peut permettre à un attaquant de perturber le bon fonctionnement de l'appliance, sans compromettre la sécurité du système.

Description

Plusieurs erreurs d'implémentation dans le composant OpenSSH peuvent permettre à un attaquant de provoquer un Déni de service lors de l'établissement de connexions SSH sur l'appliance.

Cela nécessite que l'attaquant soit autorisé à établir des connexions SSH sur l'appliance, par le biais d'un accès d'administration.

Impact

L'attaquant peut faire consommer inutilement des ressources CPU ou faire arrêter inopinément le processus, perturbant ainsi le bon fonctionnement du daemon SSH.

Gravité

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

- Déni de service sur le daemon SSH ;
- Exploitation possible uniquement depuis un réseau autorisé.



Références

- OpenSSH 4.4 (<http://article.gmane.org/gmane.network.openssh.announce/41>)
- CVE-2006-5051 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5051>)

Versions impactées

Version majeure 1.0 : non impactée

Version majeure 2.0 : <= 2.0/2

Solution

La version SSL360 2.0/3 comporte 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

