

Vulnérabilité dans la vérification des signatures RSA par le composant OpenSSL

Date de découverte	05 Septembre 2006
Révision du bulletin	AK-2006-04 1.1 (22 Septembre 2006)
Gravité	Moyenne
Impact	Contournement de la politique de sécurité
Niveau de compétence requis de l'attaquant	Expert
Provenance de l'attaque	Internet
Popularité	Haute
Versions SSL360 concernées	Toutes avant 2.0/3

Introduction

Une vulnérabilité a été découverte dans le composant OpenSSL utilisé lors de la vérification des signatures RSA dans le produit SSL360. Son exploitation peut permettre à un attaquant de contourner la politique de sécurité concernant la vérification des chaînes de confiance des certificats X.509.

Seules les configurations utilisant un certificat provenant d'une PKI pour l'appliance SSL360 sont potentiellement impactées.

Se référer à la section '*Comment détecter les configurations impactées ?*' de ce bulletin pour déterminer si vous êtes impactés.

Description

Dans une configuration utilisant une autorité de certification, le certificat X.509 d'un utilisateur doit être vérifié par l'appliance SSL360 en utilisant le certificat du CA¹ afin de s'assurer qu'il est légitime.

Une erreur d'implémentation peut permettre à un attaquant de faire accepter un certificat forgé, celui-ci étant considéré comme signé par l'autorité de certification, lorsque celle-ci utilise une clé RSA avec un exposant de 3. L'authentification par mot de passe reste toutefois obligatoire.

Note : ce type de clé est peu répandu, de plus, le certificat par défaut de l'appliance SSL360 et les autorités de certification générées par les appliances UTM FAST360 n'utilisent pas ce type d'exposant.

¹ Autorité de certification



Impact

Dans une configuration où l'authentification des certificats utilisateurs est activée et que le certificat du CA utilise une clé RSA avec un exposant de 3, cette vulnérabilité peut permettre à une personne mal intentionnée de contourner la vérification des certificats et d'accéder à la fenêtre d'authentification.

Gravité

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

- contournement de la politique de sécurité (authentification du certificat) ;
- ne permet pas l'authentification sur l'apppliance SSL360 sans connaissance du mot de passe de l'utilisateur.

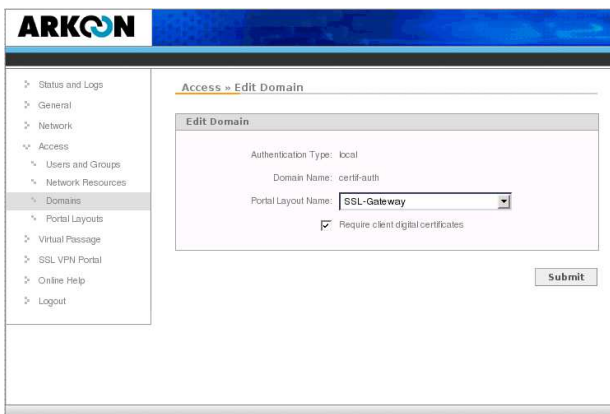
Comment détecter les configurations impactées ?

Versions impactées :

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

Configurations impactées :

- Vérification des certificats utilisateurs activée auprès d'une PKI utilisant une clé RSA avec un exposant de 3.



Activation de la vérification des certificats utilisateurs

```
# openssl x509 -in /var/httpd/cacerts/cacerts.pem -noout -text
...
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:b6:1b:3d:8a:b7:24:18:21:4c:c5:07:26:b5:2d:
    a4:2d:26:ef:5f:dc:66:91:1d:53:dc:86:06:19:d3:
    50:4a:75:1d:9d:18:80:d8:0d:af:16:db:dd:2b:07:
    fe:a4:7b:c1:ef:45:7f:1b:6a:1b:7b:ae:24:4b:1f:
    43:bc:42:0b:08:ac:12:4c:c8:42:47:72:50:fc:ce:
    68:14:b9:9d:c4:4e:d1:1e:c5:74:9b:9d:15:b4:cb:
    b9:1c:e5:90:6e:f8:e0:97:76:00:f3:cf:34:75:22:
    df:71:04:96:79:cb:54:1b:ff:e9:89:d1:44:17:a3:
    b5:c9:56:6f:d7:1d:e6:27:df
  Exponent: 3 (0x3)
...
```

Certificat du CA utilisé par la PKI utilisant une clé RSA avec un exposant de 3

Références

- OpenSSL Security Advisory (http://www.openssl.org/news/secadv_20060905.txt)
- CVE-2006-4339 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339>)



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

