



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 08 septembre 2004
N° CERTA-2004-AVI-305

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de OpenCA

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-2004-AVI-305>

Gestion du document

Référence	CERTA-2004-AVI-305
Titre	Vulnérabilité de OpenCA
Date de la première version	08 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenCA du 06 septembre 2004
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

Cross Site Scripting (XSS).

2 Systèmes affectés

- Pour la branche stable, OpenCA version 0.9.1-8 et versions antérieures ;
- pour la branche de développement, OpenCA version 0.9.2 RC6 et versions antérieures.

3 Résumé

Une vulnérabilité dans OpenCA permet à un utilisateur mal intentionné d'injecter du code malicieux dans une page HTML.

4 Description

OpenCA est une autorité de certification Open Source basée sur de nombreux produits du monde du logiciel libre tels OpenLDAP, OpenSSL, Apache et Apache mod_ssl.
Une vulnérabilité de type Cross Site Scripting (XSS) permet à un utilisateur mal intentionné d'injecter du code HTML malicieux.

5 Solution

- Pour la branche stable, mettre à jour OpenCA en version 0.9.1-9 ou supérieure ;
- pour la branche de développement, mettre à jour OpenCA via CVS.

Site Internet de téléchargement de OpenCA :
<http://www.openca.org/openca/downloads.shtml>

6 Documentation

- Site Internet de OpenCA :
<http://www.openca.org/openca/>
- Bulletin de sécurité OpenCA du 06 septembre 2004 :
<http://www.openca.org/news/CAN-2004-0787.txt>
- Référence CVE CAN-2004-0787 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0787>

Gestion détaillée du document

08 septembre 2004 version initiale.