



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 24 décembre 2009  
N° CERTA-2009-AVI-557-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans OSSIM

---

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-2009-AVI-557>

---

### Gestion du document

Référence	CERTA-2009-AVI-557-001
Titre	Vulnérabilités dans OSSIM
Date de la première version	21 décembre 2009
Date de la dernière version	24 décembre 2009
Source(s)	
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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

OSSIM version 2.1.5-3 et version précédentes.

## 3 Résumé

Plusieurs vulnérabilités affectent OSSIM et permettent à un utilisateur malveillant de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités affectent OSSIM (Open Source Security Information Management) :

- un manque de vérification dans le script `repository_attachment.php` permet à un utilisateur malveillant de charger à distance un fichier arbitraire à la racine du site et d'exécuter du code PHP ;

- un manque de validation de certaines variables permet à un utilisateur malveillant d'exécuter des commandes à distance ;
- un manque de vérification dans le script *repository\_attachment.php* permet à un utilisateur malveillant d'injecter ou de modifier des requêtes SQL.

## 5 Solution

La version 2.1.5-4 remédie à ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Annonce de la version OSSIM 2.1.5-4 du 16 décembre 2009 :  
<http://www.alienvault.com/community.php?section=News>
- Site de téléchargement du projet OSSIM :  
<http://www.sourceforge.net/projects/os-sim/>
- Référence CVE CVE-2009-4372 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4372>
- Référence CVE CVE-2009-4373 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4373>
- Référence CVE CVE-2009-4374 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4374>
- Référence CVE CVE-2009-4375 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4375>

## Gestion détaillée du document

**21 décembre 2009** version initiale.

**24 décembre 2009** ajout des références CVE.