

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans SquirrelMail

---

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-2006-AVI-229>

---

### Gestion du document

Référence	CERTA-2006-AVI-229-002
Titre	Vulnérabilité dans SquirrelMail
Date de la première version	07 juin 2006
Date de la dernière version	02 août 2006
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

Atteinte à la confidentialité des données.

## 2 Systèmes affectés

Tout système utilisant SquirrelMail en version antérieure à la 1.4.6.

## 3 Résumé

Un utilisateur distant mal intentionné peut accéder au contenu des fichiers du système hôte à l'aide d'une adresse réticulaire (« URL ») habilement construite.

## 4 Description

SquirrelMail est un service de messagerie (support IMAP et SMTP) accessible au travers d'une interface « Web ». Il est codé en utilisant le langage de script PHP.

Une mauvaise validation des entrées permet d'inclure des fichiers spécifiés par l'utilisateur. Cela induit donc un risque d'atteinte à la confidentialité des données.

## 5 Solution

Mettre à jour les sources en version 1.4.6 au moins. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Site internet de SquirrelMail :  
<http://www.squirrelmail.org>
- Bulletin de sécurité SquirrelMail du 01 juin 2006 :  
<http://www.squirrelmail.org/security/issue/2006-06-01>
- Bulletin de sécurité Red Hat RHSA-2006-0547 du 03 juillet 2006 :  
<http://rhn.redhat.com/errata/RHSA-2006-0547.html>
- Bulletin de sécurité SGI 20060703-01-P du 31 juillet 2006 :  
<ftp://patches.sgi.com/support/free/security/advisories/20060703-01-U.asc>
- Référence CVE CVE-2006-2842 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2842>

## Gestion détaillée du document

**07 juin 2006** version initiale.

**06 juillet 2006** ajout de la référence CVE et du bulletin de sécurité Red Hat.

**02 août 2006** ajout de la référence au bulletin de sécurité SGI.