Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2007
N° CERTA-2006-AVI-526-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans SquirrelMail

Gestion du document

Référence	CERTA-2006-AVI-526-002
Titre	Vulnérabilités dans SquirrelMail
Date de la première version	04 décembre 2006
Date de la dernière version	26 mars 2007
Source(s)	Bulletin de sécurité SquirrelMail du 02 décembre 2006
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

Attaque de type `Cross Site Scripting`.

2 Systèmes affectés

Toute version de SquirrelMail antérieures à 1.4.9a.

3 Résumé

Deux vulnérabilités dans SquirrelMail permettent à un utilisateur distant de réaliser une attaque de type `Cross Site Scripting`.

4 Description

Ces vulnérabilités sont causées par un manque de contrôle sur les arguments retournés à l'utilisateur et par une erreur dans le filtre `HTML magicHTML`. Les scripts `PHP` vulnérables, `webmail.php` et `compose.php`, sont exécutés depuis les menus `draft`, `compose` et `mailto`. Un utilisateur distant peut exploiter ces vulnérabilités afin d'injecter du code arbitraire depuis le serveur (sain) et l'exécuter dans le contexte du navigateur Internet de l'utilisateur connecté.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité SquirrelMail du 02 décembre 2006 :
  http://squirrelmail.org/security/issue/2006-12-02
- Note de changement de version SourceForge 468482 :
  http://sourceforge.net/project/shownotes.php?release_id=468482
- Bulletion de sécurité RedHat RHSA-2007:0022 du 31 janvier 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-002.html
- Bulletion de sécurité Debian DSA-1241 du 25 décembre 2006 :
  http://www.debian..org/security/2006/dsa-1241
- Bulletion de sécurité SuSE SUSE-SR:2006:029 du 19 décembre 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Dec/0008.html
- Bulletion de sécurité SuSE SUSE-SR:2007:004 du 16 mars 2007 :
  http://lists.suse.com/archive/suse-security-announce/2007-Mar/0005.html
- Référence CVE CVE-2006-6142 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6142

Gestion détaillée du document

04 décembre 2006 version initiale.
02 février 2007 ajout des références aux bullentins de sécurité RedHat, Debian et SuSE.
26 mars 2007 ajout de la référence au bulletin de sécurité SuSE.