Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2006
N° CERTA-2006-AVI-351-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de SquirrelMail

Gestion du document

Référence	CERTA-2006-AVI-351-003
Titre	Vulnérabilité de SquirrelMail
Date de la première version	11 août 2006
Date de la dernière version	28 septembre 2006
Source(s)	Bulletin de sécurité du projet SquirrelMail
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Les versions de SquirrelMail comprises entre 1.4.0 et 1.4.7 (incluses).

3 Description

SquirrelMail est un outil de *webmail* écrit en PHP4, et permettant d'intéragir avec les protocoles IMAP et SMTP. Une vulnérabilité a été identifiée dans la fonction `compose.php`. Cette dernière permet de restaurer le message en cours d'écriture quand la session de l'utilisateur expire.

Une personne malveillante authentifiée sur le système peut profiter de cette vulnérabilité pour lire ou écrire dans certaines variables, et ainsi accéder à certaines options de l'utilisateur ou à des documents stockés en pièce jointe.

4 Solution

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

5 Documentation

- Référence CVE CVE-2006-4019 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4019
- Site officiel du projet SquirrelMail :
  http://www.squirrelmail.org
- Bulletin de sécurité FreeBSD :
  http://www.vuxml.org/freebd/index.html
- Bulletin de sécurité Debian DSA-1154 du 20 août 2006 :
  http://www.debian.org/security/2006/dsa-1154
- Bulletin de sécurité SuSE SUSE-SA:2006:023 du 27 septembre 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Sep/0011.html
- Bulletin de sécurité Red Hat RHSA-2006:0668 du 25 septembre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0668.html
- Bulletin de sécurité du 11 août 2006 de SquirrelMail :
  http://www.squirrelmail.org/security/issue/2006-08-11

Gestion détaillée du document

11 août 2006 version initiale ;
17 août 2006 ajout du bulletin de sécurité FreeBSD ;
23 août 2006 ajout du bulletin de sécurité Debian.
28 septembre 2006 ajout des bulletins de sécurité SuSE et Red Hat.