Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2006
N° CERTA-2006-AVI-095-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Squirrelmail

Gestion du document

Référence	CERTA-2006-AVI-095-003
Titre	Multiples vulnérabilités dans Squirrelmail
Date de la première version	28 février 2006
Date de la dernière version	13 mars 2006
Source(s)	Bulletins de sécurité SquirrelMail du 01 février 2006 Bulletins de sécurité SquirrelMail du 10 février 2006 Bulletins de sécurité SquirrelMail du 15 février 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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- attaque de type `Cross-site Scripting`.

2 Systèmes affectés

`SquirrelMail` versions 1.4.5 et antérieures.

3 Résumé

Plusieures vulnérabilités dans `SquirrelMail` permettent à un utilisateur mal intentionné de porter atteinte à l'intégrité ou à la confidentialité des données et également de réaliser une attaque de type `Cross-Site Scripting`.

4 Description

Trois vulnérabilités ont été identifiées dans `SquirrelMail` :

- La première vulnérabilité est due à un manque de contrôle du paramètre *right_main* du fichier *webmail.php*. Elle permet à un utilisateur distant mal intentionné d'injecter du code et de réaliser une attaque de type `Cross-Site Scripting` par le biais d'un courrier électronique malicieusement construit.
- La deuxième vulnérabilité est due à un manque de contrôle dans le traitement des lignes de commentaires dans les zones de définition de styles. Elle permet à un utilisateur distant d'injecter du code et de réaliser une attaque de type `Cross-Site Scripting` par le biais d'un courrier électronique malicieusement construit.
- La dernière vulnérabilité est due à un manque de contrôle du paramètre *sqimap_mailbox_select*. Elle permet à un utilisateur local et identifié d'exécuter des commandes `IMAP` ou `SMTP` arbitraires et de porter ainsi atteinte à l'intégrité ou la confidentialité des données présentes dans les comptes de messagerie.

5 Solution

La version CVS de `SquirrelMail` corrige le problème.

6 Documentation

- Site de SquirrelMail :
  http://www.squirrelmail.org
- Bulletin de sécurité SquirrelMail du 01 février 2006 :
  http://www.squirrelmail.org/security/issue/2006-02-01
- Bulletin de sécurité SquirrelMail du 10 février 2006 :
  http://www.squirrelmail.org/security/issue/2006-02-10
- Bulletin de sécurité SquirrelMail du 15 février 2006 :
  http://www.squirrelmail.org/security/issue/2006-02-15
- Bulletin de sécurité Mandriva du 27 février 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:049
- Bulletin de sécurité FreeBSD pour squirrelmail du 24 février 2006 :
  http://www.vuxml.org/freebsd/pkg-squirrelmail.html
- Bulletin de sécurité Debian DSA-988 du 08 mars 2006 :
  http://www.debian.org/security/2006/dsa-988
- Bulletin de sécurité SUSE SUSE-SR:2006:005 du 03 mars 2006 :
  http://www.novell.com/linux/security/advisories/2006_05_sr.html
- Bulletin de sécurité Gentoo GLSA 200603-09 du 12 mars 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200603-09.xml
- Référence CVE CVE-2006-0188 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0188
- Référence CVE CVE-2006-0195 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0195
- Référence CVE CVE-2006-0377 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0377

Gestion détaillée du document

28 février 2006 version initiale.
08 mars 2006 ajout de la référence au bulletin de sécurité FreeBSD.
09 mars 2006 ajout de la référence au bulletin de sécurité Debian.
13 mars 2006 ajout des références aux bulletins de sécurité SUSE et Gentoo.