

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-262>

Gestion du document

Référence	CERTA-2005-AVI-262-002
Titre	Vulnérabilité de SquirrelMail
Date de la première version	15 juillet 2005
Date de la dernière version	19 septembre 2005
Source(s)	Bulletin de sécurité Debian DSA-756 du 13 juillet 2005
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 ;
- cross-site scripting.

2 Systèmes affectés

Les versions de SquirrelMail comprises entre la version 1.4.0 et la version 1.4.5-RC1 (incluse).

3 Description

Une vulnérabilité dans SquirrelMail (mauvais filtrage de la variable `$_POST` dans le fichier `options_identities.php`) permet à un utilisateur mal intentionné de modifier des préférences des utilisateurs, de réaliser des attaques de type cross-site scripting ou d'écrire dans des fichiers arbitraires sur le système vulnérable.

4 Solution

Mettre à jour SquirrelMail en version 1.4.5.

SquirrelMail peut se télécharger à l'adresse suivante :

<http://www.squirrelmail.org/download.php>
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de SquirrelMail :
<http://www.squirrelmail.org>
- Bulletin de sécurité SquirrelMail du 13 juillet 2005 :
<http://www.squirrelmail.org/security/issue/2005-07-13>
- Bulletin de sécurité Debian DSA-756 du 13 juillet 2005 :
<http://www.debian.org/security/2005/dsa-756>
- Bulletin de sécurité SUSE SUSE-SR:2005:018 du 28 juillet 2005 :
http://www.novell.com/linux/security/advisories/2005_18_sr.html
- Bulletin de sécurité FreeBSD pour squirrelmail et ja-squirrelmail du 17 septembre 2005 :
<http://www.vuxml.org/freebsd/pkg-squirrelmail.html>
<http://www.vuxml.org/freebsd/pkg-ja-squirrelmail.html>
- Référence CVE CAN-2005-2095 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2095>

Gestion détaillée du document

15 juillet 2005 version initiale.

29 juillet 2005 ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:018.

19 septembre 2005 ajout de la référence au bulletin de sécurité FreeBSD.