



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2005
N° CERTA-2005-AVI-224-004

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-224>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-AVI-224-004 |
| Titre | Vulnérabilité de SquirrelMail |
| Date de la première version | 17 juin 2005 |
| Date de la dernière version | 29 juillet 2005 |
| Source(s) | Bulletin de sécurité SquirrelMail du 15 juin 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.

2 Systèmes affectés

Toutes les versions de SquirrelMail comprises entre 1.4.0 et 1.4.4 (version incluse).

3 Description

Plusieurs vulnérabilités dans SquirrelMail permettent à un utilisateur mal intentionné, via une URL malicieuse ou un message électronique, de réaliser des attaques de type cross-site scripting.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Un correctif pour la version 1.4.4 est disponible à l'adresse suivante :

<http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch?download>

5 Documentation

- Site Internet de SquirrelMail :
<http://www.squirrelmail.org>
- Bulletin de sécurité SquirrelMail du 15 juin 2005 :
<http://www.squirrelmail.org/security/issue/2005-06-15>
- Bulletin de sécurité FreeBSD pour squirrelmail et ja-squirrelmail du 18 juin 2005 :
<http://www.vuxml.org/freebsd/pkg-squirrelmail.html>
- Bulletin de sécurité Gentoo GLSA 200506-19 du 21 juin 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200506-19.xml>
- 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
- Référence CVE CAN-2005-1769 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1769>

Gestion détaillée du document

17 juin 2005 version initiale.

20 juin 2005 ajout de la référence au bulletin de sécurité FreeBSD.

22 juin 2005 ajout de la référence au bulletin de sécurité Gentoo.

15 juillet 2005 ajout de la référence au bulletin de sécurité Debian.

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