

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2008-AVI-579>

Gestion du document

Référence	CERTA-2008-AVI-579
Titre	Vulnérabilité dans SquirrelMail
Date de la première version	04 décembre 2008
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 1.4.17 de 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

Injection de code indirecte.

2 Systèmes affectés

SquirrelMail versions 1.4.16 et antérieures.

3 Résumé

Une vulnérabilité présente dans SquirrelMail permet à un utilisateur distant de conduire une attaque de type injection de code indirecte (*Cross-site scripting*).

4 Description

Une erreur est présente dans SquirrelMail. Elle est due à un manque de contrôle du code HTML inclus dans certains courriels. Il est donc possible à un utilisateur distant malintentionné de conduire une attaque de type injection de code indirecte par le biais d'un courriel construit de façon particulière ouvert par un utilisateur du SquirrelMail vulnérable.

NB : l'option *Show HTML Version by Default* devra être activée dans les paramètres d'affichage pour que l'exploitation de cette vulnérabilité réussisse.

5 Solution

La version 1.4.17 de SquirrelMail corrige le problème :

<http://www.squirrelmail.org/download>

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

6 Documentation

- Site de SquirrelMail :
<http://www.squirrelmail.org>
- Liste des changements apportés à la version 1.4.17 de SquirrelMail :
http://sourceforge.net/project/shownotes.php?release_id=644750&group_id=311
- Référence CVE CVE-2008-2379 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2379>

Gestion détaillée du document

04 décembre 2008 version initiale.