

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2011-AVI-410>

Gestion du document

Référence	CERTA-2011-AVI-410
Titre	Vulnérabilités dans SquirrelMail
Date de la première version	25 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Fedora Fedora-2011-9309 du 13 juillet 2011
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 la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

SquirrelMail 1.x.x versions antérieures à 1.4.21.

3 Résumé

Plusieurs vulnérabilités autorisant une personne malintentionnée à injecter indirectement du code arbitraire à distance et à obtenir des informations sensibles ont été découvertes dans *SquirrelMail*.

4 Description

Plusieurs vulnérabilités affectent *SquirrelMail*. Trois d'entre elles autorisent une personne malintentionnée à injecter indirectement du code à distance :

- CVE-2010-4554 et CVE-2011-2753 : de multiples erreurs autorisent l'injection de script ou de code HTML

à distance via différents vecteurs : les boîtes de dialogue déroulantes, le plugin de correction orthographique *SquirellSpell*, la page `Index Order` et la fonction *empty trash*.

- CVE-2011-2023 : le script `functions/mime.php` ne gère pas correctement certaines balises de style autorisant ainsi une injection de script ou de code HTML ;

La dernière vulnérabilité (CVE-2010-4554) permet à une personne malveillante d'accéder à des données sensibles de l'utilisateur (telles que son mot de passe) via un vol de clic (*clickjacking*).

5 Solution

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

6 Documentation

- Bulletin de sécurité Fedora Fedora-2011-9309 du 13 juillet 2011 :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-July/062983.html>
- Référence CVE CVE-2010-4554 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4554>
- Référence CVE CVE-2010-4555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4555>
- Référence CVE CVE-2011-2023 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2023>
- Référence CVE CVE-2011-2753 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2753>

Gestion détaillée du document

25 juillet 2011 version initiale.