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 mai 2009
N° CERTA-2009-AVI-188

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans SquirrelMail

Gestion du document

Référence	CERTA-2009-AVI-188
Titre	Multiples vulnérabilités dans SquirrelMail
Date de la première version	13 mai 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité SquirrelMail du 8, 9, 10, 11, 12 mai 2009
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 ;
- exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte.

2 Systèmes affectés

SquirrelMail versions 1.4.17 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans `SquirrelMail` permettent à un utilisateur distant de contourner la politique de sécurité, de porter atteinte à la confidentialité de certaines données ou de procéder à des attaques de type injection de code indirecte.

4 Description

Plusieurs vulnérabilités sont présentes dans `SquirrelMail` :

- un manque de contrôle dans les paramètres passés dans certaines *URI* de `SquirrelMail` permet à un utilisateur distant d'exécuter du code dans le contexte du navigateur d'un utilisateur consultant un `SquirrelMail` vulnérable ;
- une erreur dans la gestion des sessions des utilisateurs permet à une personne malveillante d'usurper la session d'un autre utilisateur ;
- un manque de contrôle lors de l'affichage de certains messages électroniques permet à un utilisateur distant de surcharger certains éléments de l'interface de `SquirrelMail` pour modifier son comportement.

5 Solution

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

6 Documentation

- Bulletins de sécurité SquirrelMail :
  http://www.squirrelmail.org/security/issue/2009-05-08
  http://www.squirrelmail.org/security/issue/2009-05-09
  http://www.squirrelmail.org/security/issue/2009-05-10
  http://www.squirrelmail.org/security/issue/2009-05-11
  http://www.squirrelmail.org/security/issue/2009-05-12
- Référence CVE CVE-2009-1578 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1578
- Référence CVE CVE-2009-1579 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1579
- Référence CVE CVE-2009-1580 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1580
- Référence CVE CVE-2009-1581 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1581

Gestion détaillée du document

13 mai 2009 version initiale.