Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2005
N° CERTA-2005-AVI-038-007

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans SquirrelMail

Gestion du document

Référence	CERTA-2005-AVI-038-007
Titre	Multiples vulnérabilités dans SquirrelMail
Date de la première version	31 janvier 2005
Date de la dernière version	10 juin 2005
Source(s)	Avis de sécurité 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

- Atteinte à l'intégrité des données ;
- exécution de code arbitraire.

2 Systèmes affectés

- SquirrelMail versions 1.4.0 RC1 à 1.4.4 RC1 (vulnérabilités CAN-2005-0103 et CAN-2005-104) ;
- SquirrelMail versions 1.4.3 RC1 à 1.4.4 RC1(vulnérabilité CAN-2005-0075).

3 Résumé

Trois vulnérabilités présentes dans SquirrelMail permettent d'exécuter du code arbitraire sur le serveur ou sur le client (`Cross Site Scripting`).

4 Description

SquirrelMail est une application de type Webmail écrite en PHP4. Plusieurs vulnérabilités ont été découvertes dans SquirrelMail :

- une vulnérabilité présente dans la page `prefs.php` permet à un individu mal intentionné d'exécuter du code arbitraire sur le serveur SquirrelMail. Cette vulnérabilité affecte uniquement les personnes ayant activé la variable `register_globals` à On (vulnérabilité CAN-2005-0075) ;
- une vulnérabilité dans le traitement des variables des adresses réticulaires (URL) permet à un individu mal intentionné, via une URL judicieusement construite, d'inclure une page web malicieuse dans SquirrelMail (vulnérabilité CAN-2005-0103) ;
- une vulnérabilité de type `Cross Site Scripting` est présente dans la page `webmail.php` qui permet à un individu mal intentionné d'exécuter du code arbitraire sur les clients accédant à SquirrelMail (vulnérabilité CAN-2005-104).

5 Solution

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

6 Documentation

- Bulletin de sécurité SquirrelMail "Local file inclusions un prefs.php" du 14 janvier 2005 :
  http://www.squirrelmail.org/security/issue/2005-01-14
- Bulletin de sécurité SquirrelMail "Frame content changing in webmail.php" du 19 janvier 2005 :
  http://www.squirrelmail.org/security/issue/2005-01-19
- Bulletin de sécurité SquirrelMail "XSS vulnerability in webmail.php" du 20 janvier 2005 :
  http://www.squirrelmail.org/security/issue/2005-01-20
- Bulletin de sécurité Gentoo GLSA 200501-39 du 28 janvier 2005 :
  http://security.gentoo.org/glsa/glsa-200501-39.xml
- Bulletin de sécurité Debian DSA-662 du 01 février 2005 :
  http://www.debian.org/security/2005/dsa-662
- Bulletin de sécurité RedHat (v.3) RHSA-2005:135 du 10 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-135.html
- Bulletin de sécurité RedHat (v.4) RHSA-2005:099 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-099.html
- Mise à jour de sécurité des paquetages NetBSD squirrelmail et ja-squirrelmail :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/squirrelmail/README.html
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/ja-squirrelmail/README.html
- Bulletin de sécurité SUSE SUSE-SR:2005:014 du 07 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_14_sr.html
- Bulletin de sécurité FreeBSD pour squirrelmail et ja-squirrelmail du 01 juin 2005 :
  http://www.vuxml.org/freebsd/pkg-squirrelmail.html
- Référence CVE CAN-2005-0075 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0075
- Référence CVE CAN-2005-0103 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0103
- Référence CVE CAN-2005-0104 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0104
- Référence CVE CAN-2005-0152 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0152

Gestion détaillée du document

31 janvier 2005 version initiale.

01 février 2005 ajout de la référence au bulletin de sécurité Debian DSA-662 et de la référence CVE CAN-2005-0152.

02 février 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200501-39.

11 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:135.

17 février 2005 ajout de la référence à un second bulletin de sécurité RedHat, RHSA-2005:099.

01 mars 2005 ajout de la référence au bulletin de sécurité NetBSD.

08 juin 2005 ajout de la référence au bulletin de sécurité SUSE.

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