



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 septembre 2004
N° CERTA-2004-AVI-263-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2004-AVI-263>

Gestion du document

Référence	CERTA-2004-AVI-263-001
Titre	Multiples vulnérabilités dans SquirrelMail
Date de la première version	04 août 2004
Date de la dernière version	08 septembre 2004
Source(s)	Bulletin de sécurité DSA-535 de Debian
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

- Exécution de code arbitraire ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- SquirrelMail version 1.4.2 (vulnérabilité CVE CAN-2004-0519) ;
- SquirrelMail version antérieures à 1.4.3 (vulnérabilité CVE CAN-2004-0520) ;
- SquirrelMail version antérieures à 1.4.3 RC1 (vulnérabilité CVE CAN-2004-0521) ;
- SquirrelMail version 1.2.10 et antérieures (vulnérabilité CVE CAN-2004-0639).

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans différentes versions de SquirrelMail.

4 Description

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

- Plusieurs vulnérabilités de type `Cross Site Scripting` permettent à un individu mal intentionné d'exécuter du code arbitraire à distance, de voler les informations d'authentification ou d'atteindre à l'intégrité des données (vulnérabilité CVE CAN-2004-0519 , CVE CAN-2004-0520 et CVE CAN-2004-0639) ;
- une vulnérabilité de type `injection SQL` permet à un individu mal intentionné d'exécuter une requête SQL non sollicitée (vulnérabilité CVE CAN-2004-0521) ;

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA-535 du 2 août 2004 :
<http://www.debian.org/security/2004/dsa-535>
- Bulletin de sécurité Gentoo GLSA 200406-08 du 15 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-08.xml>
- Bulletin de sécurité RedHat RHSA-2004:240-06 du 14 juin 2004 :
<http://www.redhat.com/errata/RHSA-2004-240.html>
- Bulletin de sécurité Apple du 07 septembre 2004 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-0519 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0519>
- Référence CVE CAN-2004-0520 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0520>
- Référence CVE CAN-2004-0521 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0521>
- Référence CVE CAN-2004-0639 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0639>
- Note d'information CERTA-2002-INF-001 du CERTA sur le Cross Site Scripting :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/>

Gestion détaillée du document

04 août 2004 version initiale.

08 septembre 2004 ajout de la référence au bulletin de sécurité Apple.