

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans RoundCube

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-198>

Gestion du document

Référence	CERTA-2011-AVI-198
Titre	Vulnérabilités dans RoundCube
Date de la première version	11 avril 2011
Date de la dernière version	–
Source(s)	Liste des modifications apportées à RoundCube 0.5.1
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 ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

Roundcube versions 0.5 et inférieures.

3 Résumé

Deux vulnérabilités ont été corrigées dans RoundCube. La première permet l'injection de requêtes illégitimes par rebond, et la seconde de contourner la politique de sécurité ce qui permet à un utilisateur malveillant d'utiliser RoundCube comme relai de messagerie.

4 Description

Une vulnérabilité permettant l'injection de requêtes illégitimes par rebond lors de la connexion a été corrigée dans RoundCube. Également, une vulnérabilité qui, lorsqu'elle est exploitée, permet à un utilisateur malveillant de contourner la politique de sécurité afin de passer des commandes illégitimes, a été corrigée.

5 Solution

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

6 Documentation

- Référence CVE CVE-2011-1492 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1492>
- Liste des modifications apportées à RoundCube 0.5.1 :
<http://trac.roundcube.net/wiki/Changelog>
- Ensemble de modification 4488 du 03 février 2011 :
<http://trac.roundcube.net/changeset/4488>
- Ensemble de modification 4490 du 03 février 2011 :
<http://trac.roundcube.net/changeset/4490>

Gestion détaillée du document

11 avril 2011 version initiale.