

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Quagga

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-2010-AVI-402>

Gestion du document

Référence	CERTA-2010-AVI-402
Titre	Vulnérabilités dans Quagga
Date de la première version	25 août 2010
Date de la dernière version	–
Source(s)	Notes de mise à jour de <i>Quagga</i> du 19 août 2010
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 à distance ;
- déni de service à distance.

2 Systèmes affectés

Serveur *Quagga* versions inférieures à 0.99.17.

3 Résumé

Des vulnérabilités dans le démon *BGP* de la suite *Quagga* permettent à un attaquant de réaliser un déni de service et d'exécuter du code arbitraire à distance.

4 Description

Une erreur de dérérérencement de pointeur *NULL* peut être exploitée pour terminer l'exécution du démon *BGP* en envoyant une requête de mise à jour spécialement constituée. Une deuxième erreur, dans le traitement des messages *Route-Refresh* peut déclencher un débordement de tampon sur le tas via un enregistrement *ORF* envoyé

par un poste déjà configuré. Une exploitation de ce débordement peut mener à une exécution de code arbitraire à distance

5 Solution

La version 0.99.17 de *Quagga* contient la version corrigée du démon *BGP*.

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

6 Documentation

- Notes de mise à jour de *Quagga* du 19 août 2010 :
<http://www.quagga.net/news2.php?y=2010&m=8&d=19>

7 Gestion détaillée du document

25 août 2010 version initiale.