

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU Radius

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-2006-AVI-514>

Gestion du document

Référence	CERTA-2006-AVI-514
Titre	Vulnérabilité de GNU Radius
Date de la première version	28 novembre 2006
Date de la dernière version	–
Source(s)	
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.

2 Systèmes affectés

– GNU Radius 1.x

3 Résumé

GNU Radius est un serveur du protocole RADIUS destiné à l'authentification des utilisateurs (RFC 2138). Une vulnérabilité de l'interface SQL de GNU Radius permet à un utilisateur d'exécuter du code arbitraire à distance.

4 Description

La vulnérabilité concerne GNU Radius compilé avec le support SQL et utilisant une base de données SQL pour l'imputation (*accounting*). Ces options sont activées par défaut dans les distributions Gentoo Linux et FreeBSD.

Une chaîne de contrôle de format est construite à partir de données de l'utilisateur. Elle est transmise sans vérifications suffisantes à la fonction `sqllog()`. Un utilisateur malveillant peut, par le biais de données malicieusement construites, exécuter du code à distance dans le contexte du service (*daemon*) `radiusd`.

5 Contournement provisoire

- Basculer vers l'un des deux autres modes d'imputation, pour maintenir la fonction sans la vulnérabilité.

6 Solution

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

7 Documentation

- Version 1.4 de GNU Radius du 24 novembre 2006 :
<http://www.gnu.org/software/radius/#downloading>
- Bulletin de sécurité iDefense du 26 novembre 2006 :
<http://www.iddefense.com/application/poi/display?id=443>
- Référence CVE CVE-2006-4181 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4181>

Gestion détaillée du document

28 novembre 2006 version initiale.