



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 février 2004
N° CERTA-2004-AVI-025

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-2004-AVI-025>

Gestion du document

Référence	CERTA-2004-AVI-025
Titre	Vulnérabilité de GNU Radius
Date de la première version	09 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité iDEFENSE 02.04.04
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

Déni de service.

2 Systèmes affectés

Toutes les versions de GNU Radius antérieures à la version 1.2.

3 Résumé

Une vulnérabilité dans GNU Radius permet à un utilisateur mal intentionné de provoquer un déni de service sur le serveur Radius (service radiusd).

4 Description

GNU Radius est un serveur Radius (RFC2866). Une vulnérabilité dans les services de comptabilité du serveur radiusd permet à un utilisateur mal intentionné de provoquer un déni de service par l'envoi d'un paquet UDP malicieusement construit. Aucune authentification n'est nécessaire pour exploiter cette vulnérabilité.

5 Contournement provisoire

Dans l'attente de la mise à jour de GNU Radius, filtrer les ports utilisés par le serveur GNU Radius (par défaut 1813/UDP ou 1646/UDP) pour les opérations de comptabilité.

6 Solution

Mettre à jour GNU Radius en version 1.2 (cf. section Documentation).

7 Documentation

- Site internet de GNU Radius :
<http://www.gnu.org/software/radius/radius.html>
- Protocole Radius RFC2866 :
<http://www.ietf.org/rfc/rfc2866.txt>
- Avis de sécurité iDEFENSE 02.04.04 :
<http://www.idefense.com/application/poi/display?id=71>
- Avis de sécurité du CERT/CC VU#277396 :
<http://www.kb.cert.org/vuls/id/277396>

Gestion détaillée du document

09 février 2004 version initiale.