



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2003
N° CERTA-2003-AVI-202-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur FreeRadius

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-2003-AVI-202>

Gestion du document

Référence	CERTA-2003-AVI-202-001
Titre	Vulnérabilité du serveur FreeRadius
Date de la première version	25 novembre 2003
Date de la dernière version	16 décembre 2003
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

Déni de service.

2 Systèmes affectés

Tout système utilisant une version de *FreeRadius* jusqu'à la 0.9.2.

3 Résumé

Deux failles ont été identifiées dans le code du serveur *FreeRadius*, qui donnent la possibilité à un utilisateur mal intentionné d'arrêter le service.

4 Description

FreeRadius est une implémentation d'un serveur d'authentification supportant le protocole de transport Radius (Remote Authentication Dial In User Service - rfc2865). Ce dernier a été initialement développé pour permettre de centraliser l'authentification des utilisateurs se connectant par téléphone, typiquement chez un fournisseur d'accès.

Ses extensions permettent aujourd'hui de l'utiliser, par exemple, pour authentifier les accès à un réseau sans fil (protocole 802.1x).

Un utilisateur mal intentionné, ayant un accès réseau au serveur, peut envoyer une requête volontairement malformée qui provoquera l'arrêt du service. L'exécution de code arbitraire à distance paraît complexe, mais n'est pas à exclure.

5 Solution

Mettre à jour le serveur.

- Sources en version 0.9.3 au moins :
<http://www.freeradius.org/getting.html>
- Red Hat Entreprise Linux :
<http://rhn.redhat.com/errata/RHSA-2003-386.html>

6 Documentation

- Message original des développeurs dans la liste de diffusion *BugTraq* :
<http://archives.neohapsis.com/archives/bugtraq/2003-11/0241.html>
- Référence CVE CAN-2003-0967 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0967>

Gestion détaillée du document

25 novembre 2003 version initiale ;

16 décembre 2003 ajouts de Red Hat et de la référence CAN-2003-0967.