

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples implémentations du protocole RADIUS vulnérables

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-2002-AVI-048>

Gestion du document

Référence	CERTA-2002-AVI-048
Titre	Multiples implémentations du protocole RADIUS vulnérables
Date de la première version	05 mars 2002
Date de la dernière version	–
Source(s)	Avis CA-2002-06 du CERT/CC
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;
- déni de service.

2 Systèmes affectés

- Ascend RADIUS versions 1.16 et précédentes;
- Cistron RADIUS versions 1.6.5 et précédentes;
- FreeRADIUS versions 0.3 et précédentes;
- GnuRADIUS versions 0.95 et précédentes;
- ICRADIUS versions 0.18.1 et précédentes;
- Livingston RADIUS versions 2.1 et précédentes;
- RADIUS (anciennement Lucent RADIUS) versions 2.1 et précédentes;
- RADIUSClient versions 0.3.1 et précédentes;
- XTRADIUS 1.1-pre1 et précédentes;
- YARD RADIUS 1.0.19 et précédentes.

3 Résumé

RADIUS (Remote Authentication Dial In User Service) est un protocole utilisé pour l'identification et l'authentification de clients distants. Des vulnérabilités ont été découvertes dans certaines implémentations de ce protocole.

4 Description

Le protocole RADIUS est utilisé pour l'identification et l'authentification de clients distants. Ce protocole est décrit dans la RFC 2138. Deux vulnérabilités ont été mises en évidence dans l'implémentation de certains serveurs RADIUS:

- Un individu mal intentionné peut effectuer à distance un débordement de mémoire et exécuter du code arbitraire. Cette vulnérabilité n'est exploitable que si l'attaquant connaît la clé secrète partagée entre le client et le serveur.
- L'envoi de paquets mal formés à destination du serveur peut causer un deni de service.

5 Solution

Se référer à l'avis CA-2002-06 du CERT/CC (cf. Documentation) pour obtenir la liste des systèmes affectés et les correctifs disponibles.

6 Documentation

Avis de sécurité CA-2002-06 "Vulnerabilities in Various Implementations of the RADIUS Protocol" du CERT/CC:

<http://www.cert.org/advisories/CA-2002-06.html>

Gestion détaillée du document

05 mars 2002 version initiale.