

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mauvaise gestion de l'authentification Radius sous OpenBSD

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-346>

Gestion du document

Référence	CERTA-2004-AVI-346
Titre	Mauvaise gestion de l'authentification Radius sous OpenBSD
Date de la première version	15 octobre 2004
Date de la dernière version	–
Source(s)	Correctif de sécurité OpenBSD du 20 septembre 2004
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

- Accès illégitime au système ;
- usurpation d'identité.

2 Systèmes affectés

OpenBSD 3.4 et 3.5 (versions antérieures non maintenues).

3 Résumé

Lorsque l'authentification de l'accès à un système *OpenBSD* est déléguée à un serveur *Radius*, un individu mal intentionné peut fabriquer une fausse réponse de ce serveur qui sera cependant validée par le système *OpenBSD* vulnérable, et ainsi accéder à l'hôte.

4 Description

Le système d'authentification ("login") d'*OpenBSD* peut être configuré pour utiliser divers schémas de validation des données d'authentification. Bien que cela ne soit pas activé par défaut, cette validation peut être confiée à un serveur distant *Radius*.

Le protocole *Radius* nécessite le partage d'un secret entre le système émetteur et le serveur *Radius* pour l'authentification mutuelle de ces derniers. Cependant *OpenBSD* ne vérifie pas que la réponse du serveur utilise le secret partagé. Un individu mal intentionné, ayant accès au réseau commun aux deux systèmes, peut donc fabriquer une fausse réponse du serveur *Radius* qui sera validée et ainsi usurper l'identité d'un utilisateur légitime quelconque.

5 Solution

Se référer aux correctifs de sécurité de l'éditeur (cf. section Documentation).

6 Documentation

- Correctif de sécurité OpenBSD 3.5 du 20 septembre 2004 :
<http://www.opensbsd.org/errata.html#radius>
- Correctif de sécurité OpenBSD 3.4 du 20 septembre 2004 :
<http://www.opensbsd.org/errata34.html#radius>

Gestion détaillée du document

15 octobre 2004 version initiale.