



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 mars 2011  
N° CERTA-2011-AVI-121

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Avahi

---

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-2011-AVI-121>

---

### Gestion du document

Référence	CERTA-2011-AVI-121
Titre	Vulnérabilité dans Avahi
Date de la première version	01 mars 2011
Date de la dernière version	–
Source	Ticket d'incident Avahi 325 du 18 février 2011
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 à distance.

## 2 Systèmes affectés

Avahi, versions antérieures à la version 0.6.29.

## 3 Résumé

Une vulnérabilité dans Avahi permet à un utilisateur malveillant de provoquer un déni de service à distance.

## 4 Description

Un utilisateur malveillant peut provoquer à distance une boucle infinie par le traitement de paquets particuliers en IPv4 et en IPv6.

## **5 Solution**

La version 0.6.29 corrige le problème.

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

## **6 Documentation**

- Ticket d'incident Avahi 325 du 18 février 2011 :  
<http://www.avahi.org/ticket/325>
- Bulletin de sécurité Mandriva MDVSA-2011:037 du 24 février 2011 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:037>
- Référence CVE CVE-2011-1002 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1002>

## **Gestion détaillée du document**

**01 mars 2011** version initiale.