



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 décembre 2010  
N° CERTA-2010-AVI-587

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Exim 4

---

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-2010-AVI-587>

---

### Gestion du document

Référence	CERTA-2010-AVI-587
Titre	Vulnérabilités dans Exim 4
Date de la première version	13 décembre 2010
Date de la dernière version	–
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

- Exécution de code arbitraire à distance ;
- élévation de privilèges.

## 2 Systèmes affectés

Exim 4.x.

## 3 Résumé

Une vulnérabilité dans certaines implantations d'Exim permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

Une autre vulnérabilité dans Exim permet à un utilisateur malveillant d'élever ses privilèges.

## 4 Description

Deux vulnérabilités affectant Exim ont été publiées :

- (CVE-2010-4344) un débordement de mémoire dans certaines implantations d'Exim est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;

- (CVE-2010-4345) le compte d'utilisateur sous lequel Exim s'exécute peut voir ses droits augmentés par l'utilisation d'un fichier de configuration alternatif.

## 5 Solution

Se référer aux bulletins de sécurité des distributions pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Site du projet Exim :  
<http://www.exim.org/>
- Bulletin de sécurité Debian DSA 2131 du 10 décembre 2010 :  
<http://www.debian.org/security/2010/dsa-2131>
- Bulletin de sécurité RedHat RHSA-2010:0970 du 10 décembre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0970.html>
- Bulletin de sécurité Suse SUSE-SA:2010:059 du 13 décembre 2010 :  
<http://lists.opensuse.org/opensuse-security-announce/2010-12/msg00003.html>
- Bulletin de sécurité Ubuntu USN-1032-1 du 11 décembre 2010 :  
<http://www.ubuntulinux.org/usn/usn-1032-1>
- Référence CVE CVE-2010-4344 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4344>
- Référence CVE CVE-2010-4345 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4345>

## Gestion détaillée du document

13 décembre 2010 version initiale.