



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 mars 2010
N° CERTA-2010-AVI-123

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans sendmail pour IBM AIX

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-123>

Gestion du document

Référence	CERTA-2010-AVI-123
Titre	Vulnérabilité dans sendmail pour IBM AIX
Date de la première version	17 mars 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- IBM AIX 5.x ;
- IBM AIX 6.x.

3 Résumé

Une vulnérabilité dans `sendmail` pour IBM AIX permet à un utilisateur distant malintentionné de contourner la politique de sécurité du système.

4 Description

Une vulnérabilité dans `sendmail`, causée par une erreur dans le traitement du caractère `nul` dans le champ *Common Name* (CN), peut être exploitée par une personne malveillante afin de réaliser des attaques de type homme-au-milieu ou de contourner la politique de contrôle d'accès.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM isgIZ72510 du 09 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72510>
- Bulletin de sécurité IBM isgIZ72515 du 09 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72515>
- Bulletin de sécurité IBM isgIZ72526 du 09 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72526>
- Bulletin de sécurité IBM isgIZ72528 du 09 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72528>
- Bulletin de sécurité IBM isgIZ72539 du 09 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72539>
- Bulletin de sécurité IBM isgIZ72602 du 10 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72602>
- Bulletin de sécurité IBM isgIZ72834 du 12 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72834>
- Bulletin de sécurité IBM isgIZ72835 du 12 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72835>
- Bulletin de sécurité IBM isgIZ72836 du 12 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72836>
- Bulletin de sécurité IBM isgIZ72837 du 12 mars 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=isgIZ72837>
- Référence CVE CVE-2009-4565 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4565>

Gestion détaillée du document

17 mars 2010 version initiale.