



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 mai 2009  
N° CERTA-2009-AVI-194

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cyrus SASL

---

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-2009-AVI-194>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-194   |
| Titre                       | Vulnérabilité dans Cyrus SASL                              |
| Date de la première version | 19 mai 2009  |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité de l'US-CERT VU#238019 du 14 mai 2009 |
| 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 ;
- déni de service à distance.

## 2 Systèmes affectés

Cyrus SASL versions 2.1.22 et antérieures.

## 3 Résumé

Une vulnérabilité présente dans Cyrus SASL permet à un utilisateur malintentionné distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Cyrus SASL (Simple Authentication and Security Layer) est une bibliothèque de fonctions pouvant être utilisée par des applications afin de mettre en œuvre un mécanisme d'authentification pour divers protocoles. Une vulnérabilité de type débordement de mémoire dans une fonction de cette bibliothèque permet à un

utilisateur distant de provoquer un déni de service des applications s'appuyant sur Cyrus SASL ou d'exécuter du code arbitraire dans le contexte de ces mêmes applications.

## **5 Solution**

La version 2.1.23 corrige le problème :

<ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.23.tar.gz>

## **6 Documentation**

- Bulletin du NIST CVE-2009-0688 du 22 février 2009 :  
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-0688>
- Note de vulnérabilité de l'US-CERT VU#238019 du 15 mai 2009 :  
<http://www.kb.cert.org/vuls/id/238019>
- Référence CVE CVE-2009-0688 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0688>

## **Gestion détaillée du document**

**19 mai 2009** version initiale.