



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 juillet 2007  
N° CERTA-2007-AVI-331

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans CA Message Queuing

---

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-2007-AVI-331>

---

### Gestion du document

Référence	CERTA-2007-AVI-331
Titre	Vulnérabilité dans CA Message Queuing
Date de la première version	25 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA du 24 juillet 2007
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.

## 2 Systèmes affectés

Les logiciels suivants sur Windows et Netware sont affectés :

- Advantage Data Transport 3.0 ;
- BrightStor SAN Manager 11.1, 11.5 ;
- BrightStor Portal 11.1 ;
- CleverPath OLAP 5.1 ;
- CleverPath ECM 3.5 ;
- CleverPath Predictive Analysis Server 2.0, 3.0 ;
- CleverPath Aion 10.0 ;
- eTrust Admin 2.01, 2.04, 2.07, 2.09, 8.0, 8.1 ;
- Unicenter Application Performance Monitor 3.0, 3.5 ;
- Unicenter Asset Management 3.1, 3.2, 3.2 SP1, 3.2 SP2, 4.0, 4.0 SP1 ;
- Unicenter Data Transport Option 2.0 ;

- Unicenter Enterprise Job Manager 1.0 SP1, 1.0 SP2 ;
- Unicenter Jasmine 3.0 ;
- Unicenter Management for WebSphere MQ 3.5 ;
- Unicenter Management for Microsoft Exchange 4.0, 4.1 ;
- Unicenter Management for Lotus Notes / Domino 4.0 ;
- Unicenter Management for Web Servers 5, 5.01 ;
- Unicenter NSM 3.0, 3.1 ;
- Unicenter NSM Wireless Network Management Option 3.0 ;
- Unicenter Remote Control 6.0, 6.0 SP1 ;
- Unicenter Service Level Management 3.0, 3.0.1, 3.0.2, 3.5 ;
- Unicenter Software Delivery 3.0, 3.1, 3.1 SP1, 3.1 SP2, 4.0, 4.0 SP1 ;
- Unicenter TNG 2.1, 2.2, 2.4, 2.4.2 ;
- Unicenter TNG JPN 2.2.

### **3 Résumé**

Une vulnérabilité dans CA Message Queuing permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

### **4 Description**

Une vulnérabilité de type débordement de mémoire a été identifiée dans plusieurs produits CA au niveau du serveur CA Message Queuing (CAM / CAFT). La faille est due à un mauvais traitement de paquets spécialement conçus envoyés vers le port 3104 TCP et peut être exploitée par un attaquant pour exécuter du code arbitraire à distance.

### **5 Solution**

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

### **6 Documentation**

- Bulletin de sécurité CA du 24 juillet 2007 :  
[http://supportconnectw.ca.com/public/dto\\_transportit/infodocs/camsgquevul-secnot.asp](http://supportconnectw.ca.com/public/dto_transportit/infodocs/camsgquevul-secnot.asp)
- Référence CVE CVE-2007-0060 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0060>

### **Gestion détaillée du document**

**25 juillet 2007** version initiale.