Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 août 2005
N° CERTA-2005-AVI-318

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Computer Associates Message Queuing

Gestion du document

Référence	CERTA-2005-AVI-318
Titre	Vulnérabilités dans Computer Associates Message Queuing
Date de la première version	22 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Computer Associates du 19 août 2005
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.

2 Systèmes affectés

- Unicenter Performance Management for OpenVMS r2.4 SP3 ;
- AdviseIT 2.4 ;
- Advantage Data Transport 3.0 ;
- BrightStor SAN Manager 1.1, 1.1 SP1, 1.1 SP2, 11.1 ;
- BrightStor Portal 11.1 ;
- CleverPath OLAP 5.1 ;
- CleverPath ECM 3.5 ;
- CleverPath Predictive Analysis Server 2.0, 3.0 ;
- 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, 5.0.1 ;
- Unicenter NSM 3.0, 3.1 ;
- Unicenter NSM Wireless Network Management Option 3.0 ;
- Unicenter Remoter 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

Plusieurs vulnérabilités découvertes dans `Computer Associates Message Queuing` permettent l'exécution de code arbitraire à distance ou la réalisation d'un déni de service.

4 Description

`CAM` est un sous-composant inclus dans de nombreux produits de `Computer Associates` permettant de gérer des messages entre les applications.

`CAFT` est une application fournie avec `CAM` pour transférer des fichiers.

Trois vulnérabilités ont été découvertes dans `Computer Associates Message Queuing` (`CAM`/`CAFT`) permettant de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

5 Solution

Appliquer le correctif de Computer Associates (voir Documentation).

6 Documentation

- Bulletin de sécurité Computer Associates du 19 août 2005 :
  http://supportconnectw.ca.com/public/ca_common_docs/camsecurity_notice.asp

Gestion détaillée du document

22 août 2005 version initiale.