



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 février 2006
N° CERTA-2006-AVI-057

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Computer Associate

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-2006-AVI-057>

Gestion du document

Référence	CERTA-2006-AVI-057
Titre	Multiples vulnérabilités dans les produits Computer Associate
Date de la première version	07 février 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Computer Associate
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

Déni de service à distance.

2 Systèmes affectés

- Advantage Data Transport 3.0 ;
- BrightStor SAN Manager 1.1 ;
- BrightStor SAN Manager 1.1 SP1 ;
- BrightStor SAN Manager 1.1 SP2 ;
- BrightStor SAN Manager 11.1 ;
- BrightStor Portal 11.1 ;
- CleverPath OLAP 5.1 ;
- CleverPath ECM 3.5 ;
- CleverPath Predictive Analysis Server 2.0 ;
- CleverPath Predictive Analysis Server 3.0 ;
- CleverPath Aion 10.0 ;
- eTrust Admin 2.01 ;
- eTrust Admin 2.04 ;

- eTrust Admin 2.07 ;
- eTrust Admin 2.09 ;
- eTrust Admin 8.0 ;
- eTrust Admin 8.1 ;
- Unicenter Application Performance Monitor 3.0 ;
- Unicenter Application Performance Monitor 3.5 ;
- Unicenter Asset Management 3.1 ;
- Unicenter Asset Management 3.2 ;
- Unicenter Asset Management 3.2 SP1 ;
- Unicenter Asset Management 3.2 SP2 ;
- Unicenter Asset Management 4.0 ;
- Unicenter Asset Management 4.0 SP1 ;
- Unicenter Data Transport Option 2.0 ;
- Unicenter Enterprise Job Manager 1.0 SP1 ;
- Unicenter Enterprise Job Manager 1.0 SP2 ;
- Unicenter Jasmine 3.0 ;
- Unicenter Management for WebSphere MQ 3.5 ;
- Unicenter Management for Microsoft Exchange 4.0 ;
- Unicenter Management for Microsoft Exchange 4.1 ;
- Unicenter Management for Lotus Notes/Domino 4.0 ;
- Unicenter Management for Web Servers 5 ;
- Unicenter Management for Web Servers 5.0.1 ;
- Unicenter NSM 3.0 ;
- Unicenter NSM 3.1 ;
- Unicenter NSM Wireless Network Management Option 3.0 ;
- Unicenter Remote Control 6.0 ;
- Unicenter Remote Control 6.0 SP1 ;
- Unicenter Service Level Management 3.0 ;
- Unicenter Service Level Management 3.0.1 ;
- Unicenter Service Level Management 3.0.2 ;
- Unicenter Service Level Management 3.5 ;
- Unicenter Software Delivery 3.0 ;
- Unicenter Software Delivery 3.1 ;
- Unicenter Software Delivery 3.1 SP1 ;
- Unicenter Software Delivery 3.1 SP2 ;
- Unicenter Software Delivery 4.0 ;
- Unicenter Software Delivery 4.0 SP1 ;
- Unicenter TNG 2.1 ;
- Unicenter TNG 2.2 ;
- Unicenter TNG 2.4 ;
- Unicenter TNG 2.4.2 ;
- Unicenter TNG JPN 2.2.

Ces Produits sont vulnérables dans leurs version pour les systèmes d'exploitation suivant : AIX, DG Intel, DG Motorola, DYNIX, OSF1, HP-UX, IRIX, Linux Intel, Linux s/390, Solaris Intel, Solaris Sparc, Unix-Ware et Windows.

3 Description

Plusieurs vulnérabilités affectent le module CAM présent dans plusieurs produits de Computer Associates. Ces vulnérabilités, une fois exploitées, conduisent à un déni des service du produit concerné.

4 Solution

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

5 Documentation

- Références et correctifs de l'éditeur :
 - http://supportconnectw.ca.com/public/ca_common_docs/camessagsecurity_cam111fixes.asp
 - http://supportconnectw.ca.com/public/ca_common_docs/camessagsecurity_cam107fixes.asp
- Référence CVE CVE-2006-0529 :
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0529>
- Référence CVE CVE-2006-0530 :
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0530>

Gestion détaillée du document

07 février 2006 version initiale.