



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 novembre 2005
N° CERTA-2005-AVI-443

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Computer Associates iGateway

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-2005-AVI-443>

Gestion du document

Référence	CERTA-2005-AVI-443
Titre	Vulnérabilité dans Computer Associates iGateway
Date de la première version	08 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Computer Associates 33485 du 19 octobre 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.

2 Systèmes affectés

- Computer Associates iGateway 3.0 (versions antérieures au 23 juin 2005) ;
- Computer Associates iGateway 4.0 (versions antérieures au 23 juin 2005).

Computer Associates iGateway est inclus dans les produits suivants :

- Advantage Data Transformer (ADT) R2.2 ;
- Harvest Change Manager R7.1 ;
- BrightStor ARCserve Backup r11.5 ;
- BrightStor ARCserve Backup r11.1 ;
- BrightStor ARCserve Backup pour Windows r11 ;
- BrightStor Enterprise Backup 10.5 ;
- BrightStor ARCserve Backup v9.01 ;
- BrightStor ARCserve Backup Laptop & Desktop r11.1 ;
- BrightStor ARCserve Backup Laptop & Desktop r11 ;

- BrightStor Process Automation Manager r11.1 ;
- BrightStor SAN Manager r11.1 ;
- BrightStor SAN Manager r11.5 ;
- BrightStor Storage Resource Manager r11.5 ;
- BrightStor Storage Resource Manager r11.1 ;
- BrightStor Storage Resource Manager r6.4 ;
- BrightStor Storage Resource Manager r6.3 ;
- BrightStor Portal 11.1 ;
- eTrust Audit 1.5 SP2 (iRecorders et ARIES) ;
- eTrust Audit 1.5 SP3 (iRecorders et ARIES) ;
- eTrust Audit 8.0 (iRecorders et ARIES) ;
- eTrust Admin 8.0 ;
- eTrust Admin 8.1 ;
- eTrust Identity Minder 8.0 ;
- eTrust Secure Content Manager (SCM) R8 ;
- eTrust Web Service Security R8 ;
- eTrust Integrated Threat Management (ITM) R11 ;
- Unicenter CA Web Services Distributed Management R11 ;
- Unicenter AutoSys JM R11 ;
- Unicenter Management pour Weblogic / Management pour WebSphere R11 ;
- Unicenter Service Delivery R11 ;
- Unicenter Service Level Management (USLM) R11 ;
- Unicenter Application Performance Monitor R11 ;
- Unicenter Service Desk R11 ;
- Unicenter Service Desk Knowledge Tools R11 ;
- Unicenter Service Fulfillment 2.2 ;
- Unicenter Service Fulfillment R11 ;
- Unicenter Asset Portfolio Management R11 ;
- Unicenter Service Matrix Analysis R11 ;
- Unicenter Service Catalog/Fulfillment/Accounting R11 ;
- Unicenter MQ Management R11 ;
- Unicenter Application Server Management R11 ;
- Unicenter Web Server Management R11 ;
- Unicenter Exchange Management R11.

3 Description

Une vulnérabilité a été découverte dans le traitement des requêtes HTTP GET par *iGateway* quand le mode debug est activé. Un utilisateur mal intentionné peut, par le biais de requêtes HTTP GET malicieusement constituées, exécuter du code arbitraire à distance.

4 Solution

Mettre à jour *iGateway* en version 4.0.050623 ou supérieure.

5 Documentation

- Bulletin de sécurité 33485 de Computer Associates du 19 octobre 2005 :
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33485>
- Référence CVE CAN-2005-3190 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3190>

Gestion détaillée du document

08 novembre 2005 version initiale.