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 juin 2007
N° CERTA-2007-AVI-275-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Ingres

Gestion du document

Référence	CERTA-2007-AVI-275-001
Titre	Multiples vulnérabilités dans Ingres
Date de la première version	22 juin 2007
Date de la dernière version	25 juin 2007
Source(s)	Bulletins de sécurité Computer Associates du 21 juin 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

- Ingres 2006 version 9.0.4 ;
- Ingres r3 ;
- Ingres 2.6 ;
- Ingres 2.5.

Les versions vulnérables d'*Ingres* sont intégrées dans les produits suivants :

- Advantage Data Transformer r2.2 ;
- AllFusion Enterprise Workbench r1.1, 1.1 SP1, r7, r7.1 ;
- AllFusion Harvest Change Manager r7, r7.1 ;
- BrightStor ARCserve Backup v9 (Linux seulement), r11.1, r11.5 (Unix, Linux et Mainframe Linux) ;
- BrightStor ARCserve Backup for Laptops and Desktops r11.5 ;
- BrightStor Enterprise Backup (Unix seulement) t10.5 ;
- BrightStor Storage Command Center r11.5 ;

- BrightStor Storage Resource Manager r11.5 ;
- CleverPath Aio Business Rules Expert r10.1 ;
- CleverPath Predictive Analysis Server r3 ;
- DocServer 1.1 ;
- eTrust Admin v8, v8.1, r8.1 SP1, r8.1 SP2 ;
- eTrust Audit r8 SP2 ;
- eTrust Directory r8.1 ;
- eTrust IAM Suite r8.0 ;
- eTrust IAM Toolkit r8.0, r8.1 ;
- eTrust Identity Manager r8.1 ;
- eTrust Network Forensics r8.1 ;
- eTrust Secure Content Manager r8 ;
- eTrust Single Sign-On r7, r8, r8.1 ;
- eTrust Web Access Control 1.0 ;
- Unicenter Advanced Systems Management r11 ;
- Unicenter Asset Intelligence r11 ;
- Unicenter Asset Portfolio Management r11 r2.1, r11.3 ;
- Unicenter CCS r11 ;
- Unicenter Database Command Center r11.1 ;
- Unicenter Desktop and Server Management r11 ;
- Unicenter Desktop Management Suite r11 ;
- Unicenter Enterprise Job Manager r1 SP3, r1 SP4 ;
- Unicenter Job Management Option r11 ;
- Unicenter Lightweight Portal 2 ;
- Unicenter Management Portal r3.1.1 ;
- Unicenter Network and Systems Management r3.0, r11 ;
- Unicenter Network and Systems Management - Tiered - Multi Platform r3.0 0305, r3.1 0403, r11.0 ;
- Unicenter Patch Management r11 ;
- Unicenter Remote Control 6, r11 ;
- Unicenter Service Accounting r11, r11.1 ;
- Unicenter Service Assure r2.2, r11, r11.1 ;
- Unicenter Service Catalog r11, r11.1 ;
- Unicenter Service Delivery r11.0, r11.1 ;
- Unicenter Service Intelligence r11 ;
- Unicenter Service Metric Analysis r3.0.2, r3.5, r11, r11.1 ;
- Unicenter ServicePlus Service Desk 5.5 SP3, 6.0, 6.0 SP1, r11, r11.1, r11.2 ;
- Unicenter Software Delivery r11 ;
- Unicenter TNG 2.4, 2.4.2, 2.4.2J ;
- Unicenter Workload Control Center r1 SP3, r1 SP4 ;
- Unicenter Web Services Distributed Management 3.11, 3.50 ;
- Wily SOA Manager 7.1.

3 Résumé

De multiples vulnérabilités affectant la base de données *Ingres* permettent l'exécution de code arbitraire à distance.

4 Description

Sept vulnérabilités affectant la base de données *Ingres* ont été rendues publiques. Plusieurs de ces vulnérabilités permettent l'exécution de code arbitraire à distance, sans authentification préalable. L'exploitation d'une de ces vulnérabilités se fait par l'intermédiaire de paquets malformés envoyés aux services `iigcc` (port 10916/tcp) et `iigcd` (port 10923/tcp).

5 Solution

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

6 Documentation

- Bulletins de sécurité Computer Associates du 21 juin 2007 :
  http://supportconnectw.ca.com/public/ca_common_docs/ingresvuln_letter.asp
  http://www.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=145778
- Référence CVE-2007-3336 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3336
- Référence CVE-2007-3337 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3337
- Référence CVE-2007-3338 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3338
- Référence CVE-2007-3334 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3334

Gestion détaillée du document

22 juin 2007 version initiale.

25 juin 2007 ajout des produits affectés intégrant une version vulnérable d'Ingres, ajout des références CVE et d'un bulletin de sécurité Computer Associates.