

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Ingres

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-2008-AVI-390>

Gestion du document

Référence	CERTA-2008-AVI-390
Titre	Multiples vulnérabilités dans Ingres
Date de la première version	05 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ingres du 01 aout 2008
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Ingres 2006 release 2 (9.1.0) ;
- Ingres 2006 release 1 (9.0.4) ;
- Ingres 2.6.

Certains produits CA utilisent ce système de gestion de base de données.

3 Résumé

Plusieurs vulnérabilités découvertes dans *Ingres* permettent à une personne malintentionnée d'exécuter du code arbitraire et d'élever ses privilèges.

4 Description

Trois vulnérabilités ont été découvertes et permettent à une personne malveillante d'élever ses privilèges et d'exécuter du code arbitraire :

- une personne non authentifiée peut attribuer à un utilisateur ou un groupe propriétaire d'un journal d'événements *verifydb* des droits en lecture et en écriture ;
- une personne non authentifiée exploitant une vulnérabilité de type écrasement de pointeur peut exécuter du code arbitraire sur le serveur de base de données ;
- une personne non authentifiée peut obtenir les privilèges d'un utilisateur *Ingres*, cette vulnérabilité combinée avec la précédente peut permettre d'obtenir les droits *root*.

5 Solution

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

6 Documentation

- Bulletin de sécurité Ingres du 01 août 2008 :
<http://www.ingres.com/support/security-alert-080108.php>
- Référence CVE CVE-2008-3356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3356>
- Référence CVE CVE-2008-3357 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3357>
- Référence CVE CVE-2008-3389 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3389>

Gestion détaillée du document

05 août 2008 version initiale.