



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 avril 2007
N° CERTA-2007-AVI-164

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans SAP RFC Library

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-2007-AVI-164>

Gestion du document

Référence	CERTA-2007-AVI-164
Titre	Multiples vulnérabilités dans SAP RFC Library
Date de la première version	10 avril 2007
Date de la dernière version	–
Source(s)	Note de mise à jour de sécurité SAP 1005397 Note de mise à jour de sécurité SAP 1003908 Note de mise à jour de sécurité SAP 1003910
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 à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- SAP RFC Library 6.40 ;
- SAP RFC Library 7.00.

3 Résumé

De multiples vulnérabilités dans la bibliothèque de fonctions RFC de SAP permettraient à un utilisateur distant de réaliser des actions malveillantes.

4 Description

Plusieurs fonctions de la bibliothèque RFC de SAP sont vulnérables. Ces fonctions font partie de l'installation par défaut de SAP RFC Library :

- une vulnérabilité de la fonction RFC_SET_SERVER_PROPERTY permettrait de réaliser un déni de service en interdisant les clients de se connecter au serveur RFC (note SAP 1005397) ;
- une vulnérabilité de la fonction RFC_START_GUI permettrait à un utilisateur distant d'exécuter du code arbitraire par le biais d'un débordement de la mémoire (note SAP 1003908) ;
- une vulnérabilité de la fonction RFC_START_PROGRAM permettrait à un utilisateur distant d'obtenir des informations sur la configuration du serveur RFC et d'exécuter du code arbitraire par le biais d'un débordement de la mémoire (note SAP 1003908) ;
- une vulnérabilité de la fonction SYSTEM_CREATE_INSTANCE permettrait à un utilisateur distant d'exécuter du code arbitraire par le biais d'un débordement de la mémoire (note SAP 1003910) ;
- une vulnérabilité de la fonction TRUSTED_SYSTEM_SECURITY permettrait à un utilisateur distant d'obtenir des informations sur les comptes utilisateurs et les groupes des serveurs RFC.

5 Solution

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

6 Documentation

- Note de mise à jour de sécurité SAP 1005397 :
<http://service.sap.com/sap/support/notes/1005397>
- Note de mise à jour de sécurité SAP 1003908 :
<http://service.sap.com/sap/support/notes/1003908>
- Note de mise à jour de sécurité SAP 1003910 :
<http://service.sap.com/sap/support/notes/1003910>

Gestion détaillée du document

10 avril 2007 version initiale.