



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 20 novembre 2003  
N° CERTA-2003-AVI-197

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans SAP DB

---

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-2003-AVI-197>

---

### Gestion du document

|                             |                                      |
|-----------------------------|--------------------------------------|
| Référence                   | CERTA-2003-AVI-197                   |
| Titre                       | Multiples vulnérabilités dans SAP DB |
| Date de la première version | 20 novembre 2003                     |
| Date de la dernière version | –                                    |
| Source(s)                   | Bulletins de sécurité @stake         |
| 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 ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

- Toutes les versions de SAP DB 7.x.

## 3 Résumé

SAP DB est une mise en oeuvre libre d'un serveur de base de données. Celui-ci peut intégrer une solution d'administration à distance via une interface web.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans SAP DB et ses outils d'administration web associés permettant à un individu mal intentionné d'exécuter du code arbitraire sur le serveur, d'accéder à des pages web

d'administration sans authentification ou de récupérer des informations présentes sur le serveur.

## 5 Solution

Mettre à jour SAP DB avec la version 7.4.03.30 :  
[http://www.sapdb.org/7.4/sap\\_db\\_software.htm](http://www.sapdb.org/7.4/sap_db_software.htm)

## 6 Documentation

- Bulletin SAP DB :  
[http://www.sapdb.org/7.4/new\\_relnfo.txt](http://www.sapdb.org/7.4/new_relnfo.txt)
- Bulletins de sécurité @stake :
  - "SAP DB Privilege Escalation/Remote Code Execution" :  
<http://www.atstake.com/research/advisories/2003/a111703-1.txt>
  - "Multiple Issues with SAP DB Web-tools" :  
<http://www.atstake.com/research/advisories/2003/a111703-2.txt>
- Référence CVE CAN-2003-0938 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0938>
- Référence CVE CAN-2003-0939 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0939>
- Référence CVE CAN-2003-0940 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0940>
- Référence CVE CAN-2003-0941 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0941>
- Référence CVE CAN-2003-0942 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0942>
- Référence CVE CAN-2003-0943 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0943>
- Référence CVE CAN-2003-0944 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0944>
- Référence CVE CAN-2003-0945 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0945>

## Gestion détaillée du document

20 novembre 2003 version initiale.