

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans SAP NetWeaver

---

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-2011-AVI-426>

---

### Gestion du document

Référence	CERTA-2011-AVI-426
Titre	Multiples vulnérabilités dans SAP NetWeaver
Date de la première version	01 août 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité SAP 1548548 Bulletin de sécurité SAP 1442517 Bulletin de sécurité SAP 1543318
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

SAP NetWeaver 7.x.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans SAP NetWeaver. Elles permettent à une personne mal-intentionnée de provoquer un déni de service à distance, d'atteindre à la confidentialité des données, et d'injecter du code indirecte à distance (XSS).

## 4 Description

Trois vulnérabilités ont été découvertes dans SAP NetWeaver :

- une erreur dans `Business Communication Broker` permet de découvrir certaines informations confidentielles (comme le niveau de mise à jour ou l'adresse IP interne) ;
- une erreur dans le traitement du paramètre `txtBtdID` de `CIDXBTDDump.jsp`, `BTDDump.jsp`, et `RNIF11BTDDump.jsp`, permet d'exécuter des scripts dans le navigateur du client ;
- un débordement d'entier dans le module de traitement XML permet de stopper et de redémarrer le service `disp+work.exe`.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité SAP 1548548 :  
<https://service.sap.com/sap/support/notes/1548548>
- Bulletin de sécurité SAP 1442517 :  
<https://service.sap.com/sap/support/notes/1442517>
- Bulletin de sécurité SAP 1543318 :  
<https://service.sap.com/sap/support/notes/1543318>

## Gestion détaillée du document

01 août 2011 version initiale.