



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 janvier 2012  
N° CERTA-2012-AVI-040

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2012-AVI-040>

---

### Gestion du document

Référence	CERTA-2012-AVI-040
Titre	Vulnérabilités dans SAP NetWeaver
Date de la première version	31 janvier 2012
Date de la dernière version	–
Source(s)	Bulletins de sécurité SAP
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risques

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

SAP NetWeaver 7.x.

## 3 Résumé

Plusieurs vulnérabilités permettant à un utilisateur distant malintentionné de contourner la politique de sécurité et d'injecter indirectement du code à distance sont présentes dans *SAP NetWeaver*.

## 4 Description

Quatre vulnérabilités sont présentes dans *SAP NetWeaver*. La première concerne une faiblesse dans la gestion des accès à certaines ressources, permettant ainsi de contourner la politique de sécurité. La deuxième permet à une personne malintentionnée d'énumérer les fichiers présents sur le système, permettant ainsi le contournement de la

politique de sécurité. La troisième permet d'effectuer une injection de code à distance grâce à une faille dans le module *Text Container Administration Application*. La dernière concerne *SAP NetWeaver Business Communication Broker* et permet à une personne malintentionnée d'effectuer une injection de code indirecte à distance.

## **5 Solution**

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

## **6 Documentation**

– Bulletins de sécurité SAP :

<https://service.sap.com/sap/support/notes/1567389>

<https://service.sap.com/sap/support/notes/1591146>

<https://service.sap.com/sap/support/notes/1591749>

<https://service.sap.com/sap/support/notes/1585652>

## **Gestion détaillée du document**

**31 janvier 2012** version initiale.