

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans SAP NetWeaver Web Application Server

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-233>

Gestion du document

Référence	CERTA-2011-AVI-233
Titre	Vulnérabilités dans SAP NetWeaver, SAP Web Application Server et SAP Enterprise Portal
Date de la première version	19 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité SAP 1512134 et 1513182
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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- SAP NetWeaver 7.x ;
- SAP Web Application Server 6.x ;
- SAP Web Application Server 7.x ;
- SAP Enterprise Portal 6.x.

3 Résumé

Des vulnérabilités permettant une injection indirecte de code à distance et une atteinte à la confidentialité des données ont été découvertes dans plusieurs produits *SAP*.

4 Description

Deux vulnérabilités ont été découvertes dans différents produits *SAP*.

La première permet à une personne malintentionnée d'injecter du code à distance. Elle concerne les produits *SAP NetWeaver 7.X* et *SAP Web Application Server 6.x* et *7.x*. Elle touche les modules *ITS Mobile Start* et *ITS Mobile Test* qui ne gèrent pas correctement certaines entrées.

La seconde permet à une personne malintentionnée d'obtenir certaines informations sensibles. Elle touche les produits *SAP Enterprise Portal 6.x* et *SAP Netweaver 7.x*. Cette vulnérabilité concerne l'affichage de messages d'erreur pouvant contenir le chemin d'installation complet du module fautif. Elle est déclenchée suite à la réception de requêtes HTTP spécialement conçues.

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 1512134:
<https://service.sap.com/sap/support/notes/1512134>
- Bulletin de sécurité SAP 1513182
<https://service.sap.com/sap/support/notes/1513182>

Gestion détaillée du document

19 avril 2011 version initiale.