



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 février 2008  
N° CERTA-2008-AVI-049

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans des produits SAP

---

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-2008-AVI-049>

---

### Gestion du document

Référence	CERTA-2008-AVI-049
Titre	Vulnérabilité dans des produits SAP
Date de la première version	06 février 2008
Date de la dernière version	–
Source(s)	Note de suivi SAP 1138934
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Le programme SAP SAPSprint dont les versions sont antérieures à 1018 ;
- SAP GUI pour Windows 6.20 n'ayant pas le niveau de correctif 72 ;
- SAP GUI pour Windows 6.40 n'ayant pas le niveau de correctif 30 ;
- SAP GUI pour Windows 7.00 n'ayant pas le niveau de correctif 6.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le démon SAP1pdc dédié à l'impression et mis en œuvre dans des produits SAP. L'exploitation de certaines d'entre elles permettent à une personne malveillante distante d'exécuter du code arbitraire sur le système vulnérable.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans le démon SAPlpd dédié à l'impression et mis en œuvre dans des produits SAP comme SAP GUI pour Windows, ou SAPSprint.

Elles concernent de mauvaises implémentations liées aux fonctions `mempcy`, `sprintf` ou `strcpy`.

L'exploitation de certaines d'entre elles permettent à une personne malveillante distante d'exécuter du code arbitraire sur le système vulnérable.

## 5 Solution

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

## 6 Documentation

- Site de mise à jour SAP :  
<http://www.sap.com/index.epx>
- Référence CVE CVE-2008-0620 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0620>
- Référence CVE CVE-2008-0621 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0621>

## Gestion détaillée du document

06 février 2008 version initiale.