



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 10 juillet 2007  
N° CERTA-2007-AVI-288

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les 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-2007-AVI-288>

---

### Gestion du document

Référence	CERTA-2007-AVI-288
Titre	Multiples vulnérabilités dans les produits SAP
Date de la première version	10 juillet 2007
Date de la dernière version	–
Source(s)	
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 ;
- déni de service à distance ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- SAP Internet Communication Framework ;
- SAP NetWeaver 4.x ;
- SAP Message Server ;
- SAP Internet Graphics Service (IGS) 6.x ;
- SAP Internet Graphics Service (IGS) 7.x ;
- SAP R/3 ;
- SAP Web Application Server 6.x ;
- SAP Web Application Server 7.x ;
- SAP DB 7.x ;
- SAP RFC Library 6.x ;
- SAP RFC Library 7.x.

### 3 Description

De nombreuses vulnérabilités découvertes dans les produits SAP permettent à un utilisateur distant malintentionné de réaliser un déni de service, de porter atteinte à la confidentialité des données ou d'exécuter du code arbitraire.

### 4 Solution

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

### 5 Documentation

- Bulletins de sécurité CNSC du 17 juin 2007 :  
[http://www.csn.ch/advisory/sap01.html?\\_\\_cookie\\_try=1](http://www.csn.ch/advisory/sap01.html?__cookie_try=1)  
[http://www.csn.ch/advisory/sap02.html?\\_\\_cookie\\_try=1](http://www.csn.ch/advisory/sap02.html?__cookie_try=1)
- Bulletins de sécurité NGS Software du 05 juillet 2007 :  
<http://www.ngssoftware.com/advisories/critical-risk-vulnerability-in-sap-message-server-heap-overflow/>  
<http://www.ngssoftware.com/advisories/medium-risk-vulnerability-in-sap-internet-graphics-server/>  
<http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-sap-internet-communication-manager-dos>  
<http://www.ngssoftware.com/advisories/critical-risk-vulnerability-in-sap-db-web-server-stack-overflow/>
- Bulletins de sécurité CYBSEC du 03 avril 2007 :  
[http://www.cybsec.com/vuln/CYBSEC-Security\\_Advisory\\_SAP\\_RFC\\_SET\\_REG\\_SERVER\\_PROPERTY\\_RFC\\_Function\\_I](http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_SET_REG_SERVER_PROPERTY_RFC_Function_I)  
[http://www.cybsec.com/vuln/CYBSEC-Security\\_Advisory\\_SAP\\_RFC\\_START\\_GUI\\_RFC\\_Function\\_Buffer\\_Overflow.pdf](http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_START_GUI_RFC_Function_Buffer_Overflow.pdf)  
[http://www.cybsec.com/vuln/CYBSEC-Security\\_Advisory\\_SAP\\_RFC\\_START\\_PROGRAM\\_RFC\\_Function\\_Multiple\\_Vuln](http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_RFC_START_PROGRAM_RFC_Function_Multiple_Vuln)  
[http://www.cybsec.com/vuln/CYBSEC-Security\\_Advisory\\_SAP\\_SYSTEM\\_CREATE\\_INSTANCE\\_RFC\\_Function\\_Buffer\\_O](http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_SYSTEM_CREATE_INSTANCE_RFC_Function_Buffer_O)  
[http://www.cybsec.com/vuln/CYBSEC-Security\\_Advisory\\_SAP\\_TRUSTED\\_SYSTEM\\_SECURITY\\_RFC\\_Function\\_Inform](http://www.cybsec.com/vuln/CYBSEC-Security_Advisory_SAP_TRUSTED_SYSTEM_SECURITY_RFC_Function_Inform)
- Référence CVE CVE-2007-1914 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1914>
- Référence CVE CVE-2007-1915 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1915>
- Référence CVE CVE-2007-1916 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1916>
- Référence CVE CVE-2007-1917 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1917>
- Référence CVE CVE-2007-1918 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1918>
- Référence CVE CVE-2007-3495 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3495>
- Référence CVE CVE-2007-3496 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3496>

### Gestion détaillée du document

10 juillet 2007 version initiale.