



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 juillet 2005  
N° CERTA-2005-AVI-227-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de Cacti

---

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-2005-AVI-227>

---

### Gestion du document

Référence	CERTA-2005-AVI-227-001
Titre	Multiples vulnérabilités de Cacti
Date de la première version	23 juin 2005
Date de la dernière version	21 juillet 2005
Source(s)	Bulletin de sécurité iDEFENSE du 22 juin 2005
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.

## 2 Systèmes affectés

Cacti 0.8.6d et versions antérieures.

## 3 Description

Cacti propose une interface web à l'outil RRDTool basée sur le langage de scripts PHP.

De multiples vulnérabilités sont présentes dans Cacti :

- une vulnérabilité de type injection de commandes SQL peut être exploitée par un utilisateur distant mal intentionné afin de réaliser des requêtes SQL arbitraires sur la base de données ;
- une vulnérabilité dans les scripts `config_settings.php` et `yop_graph_header.php` peuvent être exploitées par un utilisateur distant mal intentionné afin d'exécuter du code arbitraire sur le serveur web vulnérable.

## 4 Contournement provisoire

Positionner la variable `register_globals` à `Off` afin de prévenir l'injection de code arbitraire.  
Dans l'attente de l'application des correctifs, restreindre l'accès au serveur web.

## 5 Solution

La version 0.8.6e de Cacti corrige ces vulnérabilités.

## 6 Documentation

- Annonce de la sortie de la version 0.8.6e :  
[http://www.cacti.net/release\\_notes\\_0\\_8\\_6e.php](http://www.cacti.net/release_notes_0_8_6e.php)
- Bulletin de sécurité #265 d'iDEFENSE du 22 juin 2005 :  
<http://www.idefense.com/application/poi/display?id=265>
- Bulletin de sécurité #266 d'iDEFENSE du 22 juin 2005 :  
<http://www.idefense.com/application/poi/display?id=266>
- Bulletin de sécurité #267 d'iDEFENSE du 22 juin 2005 :  
<http://www.idefense.com/application/poi/display?id=267>
- Bulletin de sécurité Gentoo GLSA 200506-20 du 22 juin 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200506-20.xml>
- Bulletin de sécurité FreeBSD du 21 juin 2005 :  
<http://www.vuxml.org/freebsd/pkg-cacti.html>
- Bulletin de sécurité Debian DSA-764 du 21 juillet 2005 :  
<http://www.debian.org/security/2005/dsa-764>
- Référence CVE CAN-2005-1524 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1524>
- Référence CVE CAN-2005-1525 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1525>
- Référence CVE CAN-2005-1526 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1526>

## Gestion détaillée du document

**23 juin 2005** version initiale.

**21 juillet 2005** ajout de la référence au bulletin de sécurité Debian DSA-764.