



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-243-003

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-243>

---

### Gestion du document

Référence	CERTA-2005-AVI-243-003
Titre	Multiples vulnérabilités de Cacti
Date de la première version	04 juillet 2005
Date de la dernière version	21 juillet 2005
Source(s)	Bulletin de vulnérabilité Hardened - PHP

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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Cacti 0.8.6e et versions antérieures.

## 3 Description

Cacti propose une interface à l'outil RRDTool qui utilise le langage de scripts PHP.  
De multiples vulnérabilités sont présentes dans Cacti :

- Une vulnérabilité permettant l'injection de code SQL dans l'URL au niveau des filtres mis en place suite aux vulnérabilités précédentes (CERTA-2005-AVI-227) peut être exploitée par un utilisateur mal intentionné afin de réaliser des requêtes arbitraires sur la base de données ;
- une vulnérabilité dans la gestion de l'URL au niveau des filtres mis en place suite aux vulnérabilités précédentes (CERTA-2005-AVI-227) peut être exploitée par un utilisateur mal intentionné afin d'injecter des commandes système ;

- une vulnérabilité dans la gestion des en-têtes HTTP peut être utilisée par un utilisateur mal intentionné afin de contourner le système d’authentification de Cacti. Ainsi, il lui est possible d’obtenir les droits d’administration et par conséquent, d’exécuter des commandes système sur le serveur web.

## 4 Solution

La version 0.8.6f de Cacti corrige ces vulnérabilités.

## 5 Documentation

- Annonce de la sortie de la version 0.8.6f  
[http://www.cacti.net/release\\_notes\\_0\\_8\\_6f.php](http://www.cacti.net/release_notes_0_8_6f.php)
- Bulletin de sécurité 03/2005 de Hardened - PHP du 01 Juillet 2005  
<http://www.hardened-php.net/advisory-032005.php>
- Bulletin de sécurité 04/2005 de Hardened - PHP du 01 Juillet 2005  
<http://www.hardened-php.net/advisory-042005.php>
- Bulletin de sécurité 05/2005 de Hardened - PHP du 01 Juillet 2005  
<http://www.hardened-php.net/advisory-052005.php>
- Bulletin de sécurité FreeBSD pour cacti du 05 juillet 2005 :  
<http://www.vuxml.org/freebsd/pkg-cacti.html>
- Bulletin de sécurité SUSE SUSE-SR:2005:017 du 13 juillet 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_17\\_sr.html](http://www.novell.com/linux/security/advisories/2005_17_sr.html)
- Bulletin de sécurité Debian DSA-764 du 21 juillet 2005 :  
<http://www.debian.org/security/2005/dsa-764>
- Référence CVE CAN-2005-2148 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2148>
- Référence CVE CAN-2005-2149 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2149>

## Gestion détaillée du document

**04 juillet 2005** version initiale.

**06 juillet 2005** ajout de la référence au bulletin de sécurité FreeBSD.

**13 juillet 2005** ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:017 et des références CVE CAN-2005-2148 et CAN-2005-2149.

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