



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 mars 2005  
N° CERTA-2004-AVI-244-007

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de PHP

---

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-2004-AVI-244>

---

### Gestion du document

Référence	CERTA-2004-AVI-244-007
Titre	Vulnérabilité de PHP
Date de la première version	15 juillet 2004
Date de la dernière version	01 mars 2005
Source(s)	Bulletin de sécurité Mandrake MDKSA-2004:068
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

- Cross site scripting;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

- PHP branche 4 : toutes les versions de PHP antérieures à la version 4.3.8 ;
- PHP branche 5 : toutes les versions de PHP antérieures à la version 5.0.0.

## 3 Résumé

Deux vulnérabilités dans PHP permettent à un utilisateur mal intentionné de réaliser du `cross site scripting` ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

## 4 Description

PHP est un langage de script permettant la réalisation de pages web dynamiques.

Deux vulnérabilités sont présentes dans php :

- Une première vulnérabilité concerne la directive `memory_limit` qui peut être déclenchée à un moment voulu. Ceci peut être utilisé par un utilisateur mal intentionné pour exécuter du code arbitraire (CAN-2004-0594) ;
- Une seconde vulnérabilité concerne la fonction `strip_tags()`. Cette fonction ne filtre pas correctement certaines balises, ce qui peut conduire un utilisateur mal intentionné à réaliser des attaques de type `cross site scripting` (CAN-2004-0595).

## 5 Solution

- Pour la branche 4 de PHP : mettre à jour PHP en version 4.3.8 ;
- pour la branche 5 de PHP : mettre à jour PHP en version 5.0.0.

PHP est téléchargeable à l'adresse suivante :

<http://www.php.net/downloads.php>

Dans tous les cas, se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Site Internet de PHP :  
<http://www.php.net>
- Liste des changements dans PHP pour la branche 4 :  
<http://www.php.net/ChangeLog-4.php>
- Liste des changements dans PHP pour la branche 5 :  
<http://www.php.net/ChangeLog-5.php>
- Bulletin de sécurité e-matters 11/2004 du 14 juillet 2004 :  
<http://security.e-matters.de/advisories/112004.html>
- Bulletin de sécurité e-matters 12/2004 du 14 juillet 2004 :  
<http://security.e-matters.de/advisories/122004.html>
- Bulletin de sécurité Mandrake MDKSA-2004:068 du 14 juillet 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:068>
- Bulletin de sécurité Gentoo GLSA 200407-13 du 15 juillet 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200407-13.xml>
- Bulletin de sécurité SUSE SUSE-SA:2004:021 du 16 juillet 2004 :  
[http://www.suse.com/de/security/2004\\_21\\_php4.html](http://www.suse.com/de/security/2004_21_php4.html)
- Bulletin de sécurité Red Hat RHSA-2004:392 du 19 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-392.html>
- Bulletin de sécurité Red Hat RHSA-2004:395 du 19 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-395.html>
- Bulletin de sécurité Debian DSA-531 du 20 juillet 2004 :  
<http://www.debian.org/security/2004/dsa-531>
- Bulletin de sécurité Debian DSA-669 du 07 février 2005 :  
<http://www.debian.org/security/2004/dsa-669>
- Bulletin de sécurité FreeBSD pour PHP du 15 juillet 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour php4 du 15 juillet 2004 :  
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité du paquetage NetBSD php4 :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/php4/README.html>

- Référence CVE CAN-2004-0594 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0594>
- Référence CVE CAN-2004-0595 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0595>

## **Gestion détaillée du document**

**15 juillet 2004** version initiale.

**16 juillet 2004** ajout de la référence au bulletin de sécurité Gentoo.

**16 juillet 2004** ajout de la référence au bulletin de sécurité SUSE.

**19 juillet 2004** ajout de la référence au bulletin de sécurité OpenBSD.

**20 juillet 2004** ajout des références aux bulletins de sécurité Red Hat.

**21 juillet 2004** ajout de la référence au bulletin de sécurité Debian DSA-531.

**08 février 2005** ajout de la référence au bulletin de sécurité Debian DSA-669.

**01 mars 2005** ajout de la référence au bulletin de sécurité NetBSD.