

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-2011-AVI-461>

---

### Gestion du document

Référence	CERTA-2011-AVI-461-001
Titre	Vulnérabilités dans PHP
Date de la première version	22 août 2011
Date de la dernière version	26 août 2011–
Sources	Annonce de la version PHP 5.3.7 du 18 août 2011 Mise en garde sur la version PHP 5.3.7 du 22 août 2011 Annonce de la version 5.3.8 du 23 août 2011
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

PHP 5.3.x.

## 3 Résumé

Plusieurs vulnérabilités affectent PHP et permettent de contourner la politique de sécurité.

## 4 Description

Plusieurs vulnérabilités affectent PHP :

- une mauvaise gestion de pointeur dans la fonction *substr\_replace* permet à un utilisateur malveillant de corrompre la mémoire et au moins de provoquer un déni de service ;

- un débordement dans la pile dans la fonction *socket\_connect* permet à un utilisateur malveillant d'exécuter du code arbitraire ;
- un défaut de traitement de certaines requêtes POST par la fonction *rfc1867\_post\_handler* permet à un utilisateur malveillant d'atteindre n'importe quel fichier du système ;
- une erreur dans l'implantation *crypt\_blowfish* provoque des collisions lors des calculs de condensés cryptographiques ;
- un dépassement de tampon mémoire est présent dans la fonction *crypt*.

## 5 Solution

La version 5.3.7 de PHP résoud ces problèmes mais introduit une régression (dans la fonction *crypt()*).

La version 5.3.8 résoud la régression introduite dans PHP 5.3.7.

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

## 6 Documentation

- Mise en garde sur la version PHP 5.3.7 du 22 août 2011 :  
<http://www.php.net/archive/2011.php#id2011-08-22-1>
- Annonce de la version PHP 5.3.7 du 18 août 2011 :  
<http://www.php.net/archive/2011.php#id2011-08-18-1>
- Annonce de la version PHP 5.3.8 du 23 août 2011 :  
<http://www.php.net/archive/2011.php#id2011-08-23-1>
- Référence CVE CVE-2011-1148 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1148>
- Référence CVE CVE-2011-1938 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1938>
- Référence CVE CVE-2011-2202 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2202>
- Référence CVE CVE-2011-2483 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2483>

## Gestion détaillée du document

**22 août 2011** version initiale.

**26 août 2011** ajout du correctif de la version 5.3.8 du 23 août 2011.