

Detectadas ocho vulnerabilidades en PHP



Hace ya varios días atrás se publico un artículo que reseñaba los 20 años de vida del lenguaje de programación web PHP y partir del mismo surgieron una serie de interrogantes sobre la efectividad de este lenguaje, que como cualquier otro no es infalible y tiene errores de seguridad, hoy compartimos 8 vulnerabilidades de PHP 5 que han sido detectadas y solucionadas.

El equipo de desarrollo de PHP ha publicado las actualizaciones para las ramas 5.5 y 5.4 de PHP que solucionan ocho vulnerabilidades que pueden ser aprovechadas para provocar denegaciones de servicio e incluso comprometer los sistemas afectados.

Gran parte de los problemas residen en errores en la extensión Fileinfo que pueden explotarse para provocar denegaciones de servicio a través de archivos CDF específicamente creados (CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480 y CVE-2014-3487).

Se ha corregido un problema (CVE-2014-3981) de uso inseguro de archivos temporales en el script de configuración, lo que podría permitir a usuarios locales sobrescribir archivos arbitrarios mediante un ataque por enlaces simbólicos.

Un desbordamiento de búfer en la función php_parserr de ext/standard/dns.c que podría permitir a servidores remotos la ejecución de código a través de registros DNS TXT modificados (CVE-2014-4049).

Por ultimo, un error (CVE-2014-3515) de confusión de tipos en ArrayObject y SPLObjectStorage de SPL (Standard PHP Library,

Biblioteca Estándar de PHP).

También se han solucionado otros problemas en el núcleo de PHP, CLI server, Date, Intl, Network, OpenSSL, SOAP y SPL.

Se recomienda actualizar cuanto antes a las nuevas versiones 5.4.30 y 5.5.14 desde :

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

Más información:

PHP 5.4.30 Release Announcement

http://www.php.net/releases/5_4_30.php

PHP 5.5.14 Release Announcement

http://www.php.net/releases/5_5_14.php

PHP 5 ChangeLog

<http://www.php.net/ChangeLog-5.php>

fuelle:jovenclub.cu