Encuentran múltiples vulnerabilidades de ejecución de código en PHP

Autor: I. Stepanenko

Fecha: Saturday 21st of September 2019 04:35:04 AM

Los mantenedores del lenguaje PHP lanzaron recientemente las últimas versiones de PHP para parchear múltiples vulnerabilidades graves en sus bibliotecas centrales y agrupadas. La más grave, podría permitir a los hackers ejecutar código arbitrario y comprometer servidores específicos.

El preprocesador de hipertexto, comúnmente conocido como PHP, es el lenguaje de programación web más popular del lado del servidor que actualmente alimenta más del 78% de Internet.

Las últimas versiones bajo distintas ramas mantenidas incluyen PHP versión 7.3.9, 7.2.22 y 7.1.32, que aborda distintas vulnerabilidades de seguridad.

Dependiendo del tipo, la ocurrencia y el uso de la base de código afectada en una aplicación PHP, la explotación exitosa de algunas de las vulnerabilidades más graves podría permitir a un atacante ejecutar código arbitrario en el contexto de la aplicación afectada con los privilegios asociados.

Por otro lado, los intentos fallidos de explotación probablemente resultarán en una condición de denegación de servicio (DoS) en los sistemas afectados.

Encuentran múltiples vulnerabilidades de ejecución de código en PHP

Autor: I. Stepanenko

Fecha: Saturday 21st of September 2019 04:35:04 AM

Las vulnerabilidades podrían dejar cientos de miles de aplicaciones web que dependen de PHP abiertas a ataques de ejecución de código, incluidos los sitios web impulsados por algunos sistemas de gestión de contenido populares como WordPress, Drupal y Typo3.

De estos, una vulnerabilidad de ejecución de código *"use-after-free"*, asignada como CVE-2019-13224, reside en Onigurama, una popular biblioteca de expresiones regulares que viene incluida con PHP, así como muchos otros lenguajes de programación.

Un atacante remoto puede explotar esta falla insertando una expresión regular especialmente diseñada en una aplicación web afectada, lo que puede conducir a la ejecución del código o causar la divulgación de información.

> "El atacante proporciona un par de un patrón de expresiones regulares y una cadena, con una codificación de varios bytes que se maneja con onig_new_deluxe()", dice Red Hat en su aviso de seguridad.

Otros defectos parcheados afectan la extensión curl, la función Exif, el Administrador de procesos FastCGI (FPM), la función Opcache y más.

Sin embargo, hasta ahora no existen informes sobre explotación de alguna de estas vulnerabilidades. El grupo de seguridad de PHP abordó las vulnerabilidades en las últimas versiones. Por lo tanto, se recomienda a los usuarios y proveedores de alojamiento que actualicen sus servidores a la última versión de PHP 7.3.9, 7.2.22 o 7.1.32.