Vulnerabilidad GHOST glibc, Afecta Aplicaciones WordPress Y PHP

Después de conocerse la **vulnerabilidad GHOST**, la cual es extremadamente peligrosa y afecta la **biblioteca glibc**, un componente ampliamente usado en la mayoría de las distribuciones de Linux, los investigadores de seguridad han descubierto que las aplicaciones PHP, incluido el Sistema de Gestión de Contenidos de WordPress, también podrían verse afectados por el bug.

«***GHOST***» es una vulnerabilidad critica (**CVE-2015-0235**), la cual ha sido anunciada esta semana por los investigadores de la empresa de seguridad **Qualys**, la cual se relaciona con un desbordamiento de búfer basado en el nombre de la **función glibc – «GetHOSTbyname().»** Los investigadores dijeron que la vulnerabilidad ha estado presente en el código glibc desde el 2000.

Aunque los principales distribuidores de Linux como **Red Hat**, **Debian** y Ubuntu, ya han actualizado su software contra la vulnerabilidad, GHOST podría ser usado por hackers contra unas cuantas aplicaciones para ejecutar remotamente código y hacerse con el control de un servidor Linux.

Las **aplicaciones PHP**, incluyendo WordPress también utilizan la función de contenedor **gethostbyname()**, lo que aumenta la posibilidad de que la vulneración sea mas alta, incluso después de varias distribuciones de Linux emitieron sus correcciones.

GHOST, Gran Problema Para WordPress

Según el investigador Marc-Alexandre Montpas de Sucuri, la vulnerabilidad GHOST podría ser un gran problema para WordPress, ya que utiliza la **función wp_http_validate_url()** para validar cada URL que existe en el pingback.

> *«…. Y lo hace mediante el uso de la **función gethostbyname()**«, escribió Montpas en publicación el miércoles. «Así que un atacante podría aprovechar este hueco para insertar una URL maliciosa que activaría un buffer overflow bug, del lado del servidor, lo que potencialmente permitiría obtener privilegios en el servidor.»*

La vulnerabilidad afecta a todas las versiones de glibc de glibc-2.17 e inferior. Sin embargo, fue parcheado en glibc-2.18 05 2013, pero no fue marcado como un problema de seguridad, por lo que la solución no ha sido lanzada en distribuciones de Linux comunes como RedHat y Ubuntu.

Cómo Comprobar Si El Sistemas Es Vulnerable

«Se trata de una vulnerabilidad bastante grave y debe ser tratada como tal», dijo Montpas. «Si tienes un servidor dedicado o servidor VPS que se ejecuta Linux, tienes que asegurarte de actualizar de inmediato.»

Sucuri también proporcionó el siguiente código PHP de prueba, que un administrador puede **ejecutar en su terminal de servidor**. Si el código devuelve un error de segmentación, entonces su servidor Linux puede ser **afectado por la vulnerabilidad GHOST**.

[php]php -r '$e="0″;for($i=0;$i<2500;$i++){$e="0$e";} gethostbyname($e);' Segmentation fault[/php]

Cómo Proteger

Hasta ahora, Debian 7, Red Hat Enterprise Linux 6 y 7, CentOS 6 y 7, y Ubuntu 12.04, han lanzado actualizaciones de software. Se recomienda a los usuarios de las distribuciones de Linux **instalar estas actualizaciones de seguridad**, seguido de un reinicio del sistema, tan pronto como sea posible.

Desactivar XML-RPC En WordPress

Si no deseas usar el **proceso de XML-RPC**, es preferible que las desactives por completo. Incluso existen **plugins de WordPress** que des habilitan totalmente los procesos XML-RPC.

Desactivar solicitudes Pingback En WordPress

También puede desactivar la función de pingback añadiendo el siguiente código al **archivo functions.php**:

[php]add_filter('xmlrpc_methods' , function($methods') { unset($methods['pingback.ping]); return $methods; }

);[/php]