Shellshock, El Nuevo Bug Que Amenaza La Seguridad De La Web

Hace algunos meses se conoció sobre el fallo de seguridad Heartbleed, el cual puso en entredicho la seguridad y privacidad de diversos servidores de grandes empresas. un **nuevo fallo de seguridad** conocido como el nuevo **bug de Bash** amenaza con poner en peligro nuevamente la web, desde grandes servidores hasta cámaras conectadas.

Bug Bash o Shellshock podría significar un desastre para las principales empresas digitales, **servidores de Internet** a pequeña escala e incluso dispositivos conectados a Internet.

El **fallo de seguridad Shellshock**, permite la ejecución de **código malicioso** de bash en el shell (sentencias que se manejan en la consola de los diferentes Sistemas Operativos) para raptar un sistema operativo y **acceder a información confidencial**.

Un articulo de la compañía de software de código abierto de **Red Hat** advirtió que «es común para una gran cantidad de programas ejecutar Bash en shell en background», y el error se «activa» cuando se añade código adicional dentro de las **líneas de código en el Bash**.

El experto en seguridad Robert Graham, ha advertido de que el **error Bash** es más grande y peligroso en comparación a Heartbleed porque «el bug interactúa con otro software de manera inesperada» y debido a que un «enorme porcentaje» de software interactúa con la shell.

«Mientras que los sistemas conocidos (como su servidor Web)

puedes ser actualizados, otros sistemas permanecen sin poder ser actualizados, seis meses después del bug de Heartbleed, cientos de miles de sistemas siguen siendo vulnerables.», según ha dicho Graham.

Ars Technica informa que la vulnerabilidad podría afectar a los **dispositivos con Unix y Linux**, así como el hardware que ejecuta **Max OS X**. Según Ars, una prueba en la versión 10.9.4 (Mavericks) de Mac, demostró que tiene «**una versión vulnerable de Bash**«.

> *I think I was wrong saying #shellshock was as big as #heartbleed. It's bigger.*
>
> *— Robert Graham (@ErrataRob) septiembre 25, 2014*

Graham también señalo que el **fallo Bash** también es particularmente peligroso para los dispositivos conectados a través del Internet de las cosas, debido a que su software está desarrollado usando **scripts de Bash**«. Del mismo modo, Graham dijo que el error ha existido desde hace «mucho, mucho tiempo» (al igual que **HeartBleed**), lo cual significa que un gran número de dispositivos antiguos, serán vulnerables. «El número de sistemas que necesitan ser parcheados, es mucho mayor que **Heartbleed**«, ha dicho Graham.

El bug de Heartbleed, el principal fallo de seguridad se conoció en abril, el cual se aprovecho de OpenSSL hace más de dos años, permitiendo bits aleatorios de la memoria para ser recuperados de los servidores afectados. El investigador de seguridad **Bruce Schneier** llama la falla «catastrófica«.

Parchando La Shell

Tod Beardsley, un gerente de ingeniería de la empresa de seguridad **Rapid7**, advirtió que a pesar de la complejidad baja, la vulnerabilidad afecta a una amplia gama de dispositivos, los cuales requieren que los administradores de sistemas apliquen parches de inmediato.

«Esta vulnerabilidad es potencialmente muy importante», dijo **Beardsley** a CNET. «Está clasificado en 10 de gravedad, lo que significa que tiene el máximo impacto, y » bajo» para la complejidad de la explotación, lo que significa que es bastante fácil, para ser utilizado por los atacantes.

«El software afectado, **Bash**, es ampliamente utilizado por lo atacantes, quienes pueden usar esta vulnerabilidad para acceder de forma remota una gran variedad de dispositivos y **servidores Web**. Utilizando esta vulnerabilidad, el atacante puede **tomar el control del sistema operativo**, y acceder a información confidencial, realizar cambios, entre otras cosas».

> *Attackers can potentially take over the operating system, access confidential information, make changes.*
>
> *Tod Beardsley*

Después de realizar una exploración en la Internet para probar la vulnerabilidad, **Graham** informó que el bug «puede fácilmente filtrar firewalls e infectar a una gran cantidad de sistemas» que según él sería «‘game over’ para grandes redes».