Todo Lo Que Necesitas Saber De Shellshock

Si pensaste que no había nada mas peligroso que HeartBleed te has equivocado ;) Como sabrán la mayoría de usuarios de la web, recientemente se conoció sobre un nuevo bug que afecta la Shell de sistemas basados en Unix y Linux. El nivel de peligro de este **nuevo bug**, esta catalogado en 10 de 10, una alta calificación. En este articulo, te mostraremos algunos puntos que debes saber De Shellshock ;)

¿Qué Es Shellshock?

El **error de seguridad** que afecta Bash, es una vulnerabilidad que puede permitir a un usuario malicioso (hacker) emitir comandos remotos a **servidores web**. Con este bug, es posible que un atacante pueda extraer información sensible, como los datos personales, bancarios, etc. En este punto queremos informar a nuestros clientes, que todos nuestros **servidores** han sido actualizados para evitar vulneraciones a causa de este bug.

El exploit **afecta a los servidores** y sistemas que usan un intérprete de lenguaje llamado Bash para procesar comandos. Algunas versiones de Linux y Unix utilizan Bash, y Mac OS X 10 Mavericks también lo usa, ya que está basado en una plataforma Unix.

La vulnerabilidad ha existido alrededor de unos 20 años, pero sólo se ha descubierto esta semana.

¿Por Qué Es Tan Peligroso

Shellshock?

Aunque el **bug de Bash** no afecta casi tantos dispositivos como Heartbleed, las consecuencias podrían ser mucho más graves. Esto se debe a que Bash permite a los atacantes **ejecutar comandos de forma remota**, mientras que **Heartbleed** sólo permitía a los intrusos **robar información de los servidores**.

«Este es sin duda muy diferente a Heartbleed y tiene un impacto mucho más grande», dijo **Narang**.

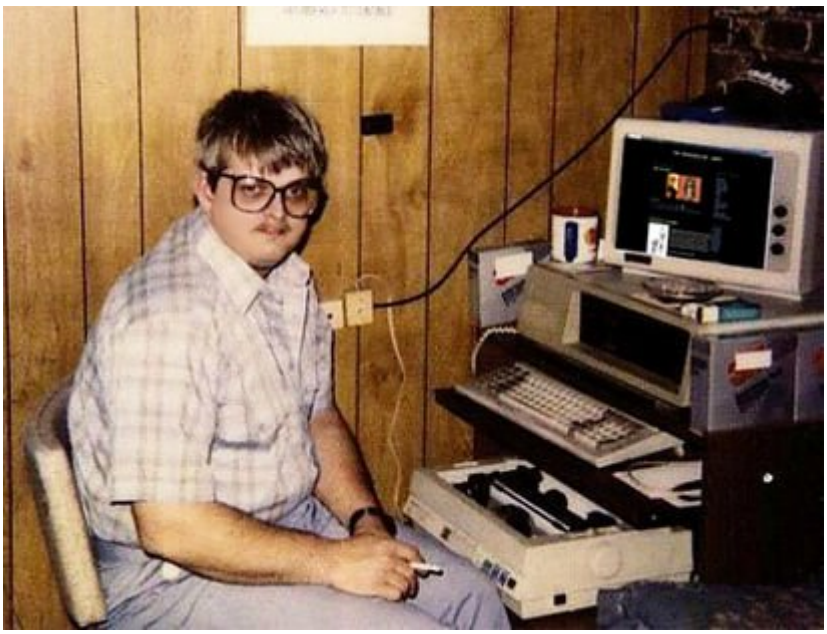
Si un pirata informático puede identificar un **servidor vulnerable**, él o ella puede realizar un número de diferentes tipos de peticiones. «El más importante es, que los hackers pueden decir al servidor en un comando, 'Hey, ¿por qué no se conecta de nuevo a mí para que yo pueda ver lo que hay en el servidor'», dijo Narang. «Ellos también pueden obtener ese servidor para devolver información de ella a través de correo electrónico.»

Uno de los mayores problemas, sin embargo, es que muchos sistemas, que no se actualizan con regularidad, no recibirán el parche necesario para corregir la vulnerabilidad. Esto puede incluir cosas como routers, que no se actualizan con

mucha frecuencia, de acuerdo con Narang.

¿Quién Debe Preocuparse Al Respecto?

El **error de Bash** también difiere de Heartbleed en que su alcance es mucho más pequeño. **Bash** no supondría ser grave para un usuario común. Pero podría tener efectos perjudiciales para cualquier empresa con una **presencia en la web**.



Lo Que Puedes Hacer Para Estar Seguro

Si eres un usuario de los Sistemas Operativos que son afectados por este bug, de seguro deseas estar al día, y hacerle frente a esta nueva vulnerabilidad. En un anterior articulo hablamos sobre como saber si eres afectado por Shellshock, ademas, de compartir algunos enlaces en los que podrás encontrar recursos para solucionar la vulnerabilidad.