Los expertos acaban de descubrir una grave falla de seguridad que le permitiría a los hackers tomar control a distancia de millones decomputadoras en todo el mundo.

Esta vulnerabilidad, bautizada como «Shellshock«, tiene más de 20 años de antigüedad, pero no salió a la luz hasta esta semana.

Ahora, la autoridad estadounidense para emergencias informáticas, el Computer Emergency Readiness Team (US-CERT), cataloga su peligrosidad con el máximo de 10 sobre 10 y les recomienda a los administradores de sistemas y a los usuarios que puedan verse afectados que apliquen inmediatamente «parches» de seguridad.

¿QUIÉN ESTÁ EN PELIGRO?

La vulnerabilidad Shellshock está dentro de un componente de software llamado Bash, un acrónimo de Bourne-Again Shell.

Bash es un programa informático que interpreta órdenes y forma parte de la plataforma Unix, sobre la que otros sistemas operativos están construidos, como Linux y el de Apple, Mac OS.

Los hackers podrían potencialmente tomar control a distancia de casi cualquier computadora o sistema que use Bash, así que esta falla de seguridad puede afectar a usuarios individuales pero también a gobiernos, bancos y autoridades militares, que pueden estar utilizando servidores de Internet que operan con el sistema Linux.

Según los expertos en seguridad, llevar a cabo ataques cibernéticosaprovechando esta vulnerabilidad es muy simple, por eso esta falla es particularmente preocupante: los criminales podrían obtener rendimientos explotando una falla de baja complejidad.

De hecho, algunos expertos creen que Shellshock es más grave que la falla Heartbleed, descubierta el pasado mes de abril.

Según Alan Woodward, investigador de seguridad de la universidad inglesa de Surrey, esta vulnerabilidad le da a un hacker un acceso directo al sistema. «La puerta está abierta de par en par», dijo.

Se estima que Shellshock podría afectar a 500 millones de usuarios. «Explotando esta vulnerabilidad, los atacantes podrían potencialmente tomar el control del sistema operativo, acceder a información confidencial, hacer cambios, etcétera», le dijo a la BBC TodBeardsley, ingeniero de la firma especialista en ciberseguridad Rapid7.

¿CÓMO PROTEGERSE?

Desafortunadamente no hay una solución rápida y efectiva para protegerse. En general, la responsabilidad de protección recae sobre los administradores de servidores y los administradores de sistemas informáticos, que tendrán que actualizar sus sistemas con los parches de seguridad adecuados.

«Cualquier persona que utilice sistemas que usan Bash necesita aplicar inmediatamente un parche de seguridad«, urgió Beardsley.

Algunos expertos advierten, sin embargo, que los parches de seguridad son «incompletos» y no podrán asegurar totalmente los sistemas.

Por su parte el investigador Alan Woodward le recomienda a los usuarios preocupados por la seguridad de sus dispositivos personales que visiten las páginas web de los fabricantes para estar pendientes de posibles actualizaciones, particularmente en lo que se refiere a dispositivos de hardware como routers. Por ahora Apple no ha ofrecido ninguna solución.

Los usuarios de Linux y Mac pueden aplicar parches individualmente, pero no es algo que cualquier individuo pueda hacer fácilmente, a pesar de que hay tutoriales en internet.

A la mayoría de los usuarios no expertos no les quedará otra que esperar a que las compañías tomen medidas.

Fuente: elcomercio