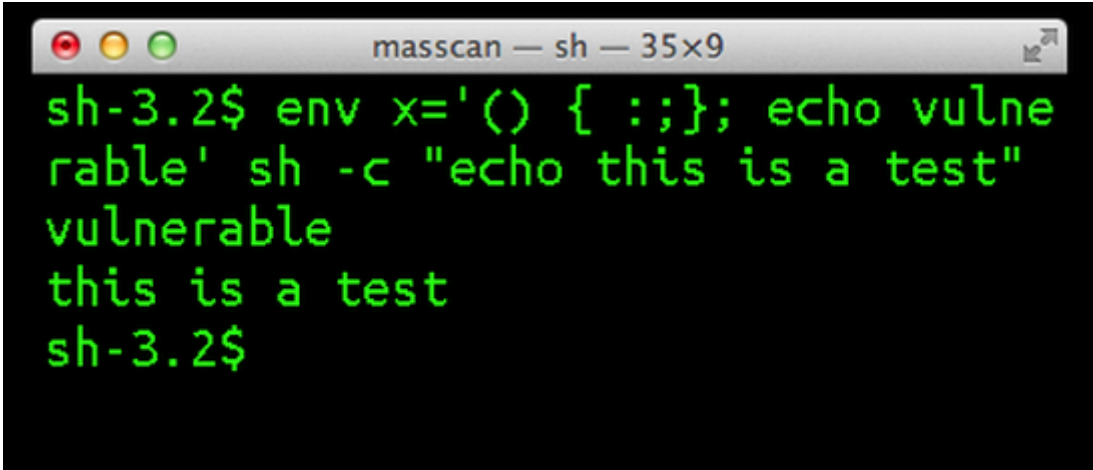


Servidores De Juegos De Yahoo Vulnerados Usando Shellshock

Como muchos ya sabrán, [Shellshock es el nuevo bug](#) que preocupa a una gran cantidad de **Webmasters**, y no es para menos, ya que este bug es mas simple de usar que [HeartBleed](#), pero mas peligroso en cuanto a la extracción de datos del servidor. El exploit de Bash ([Shellshock](#)), ha afectado a los servidores de juego de Yahoo. Pero, la compañía dice que no existen datos filtrados de clientes usando **Shellshock en los servidores**.



```
masscan — sh — 35x9
sh-3.2$ env x='() { :; }; echo vulnerable' sh -c "echo this is a test"
vulnerable
this is a test
sh-3.2$
```

La vulneración de los servidores fue [descubierta](#) por el investigador de seguridad, **Jonathan Hall**. Hall explico que dos servidores de juegos en Yahoo, habían sido vulnerados. Después de que Yahoo fue contactado por [Security Week](#), ha lanzado la siguiente declaración:

Un fallo de seguridad, llamado Shellshock, que podría exponer las vulnerabilidades en muchos servidores web fue identificado el 24 de septiembre. Tan pronto como nos dimos cuenta de la cuestión, comenzamos a parchear nuestros sistemas. Anoche, han sido aislados un puñado de nuestros servidores afectados y en este momento no tenemos ninguna evidencia de un compromiso a los datos del usuario. Estamos enfocados en brindar la experiencia más segura posible para nuestros usuarios de todo el mundo y estamos trabajando

continuamente para proteger los datos de nuestros usuarios.

El exploit es un problema de seguridad basado en Unix SSH, permite a los hackers hacerse cargo de un ordenador o servidor a través de la línea de comandos. Las empresas han estado aplicando parches de seguridad a sus servidores desde que el exploit fue descubierto. Al parecer, **Yahoo** no había tomando en cuenta sus servidores de **Yahoo Games**.