# Google Revela Tercer Vulnerabilidad Sin Parchar De Windows

Microsoft ha criticado fuertemente a Google y su política de divulgación de fallos, ya que reveló públicamente dos vulnerabilidades de día cero de Windows 8.1. Al parecer **Google no le da descanso a Microsoft**, o eso hace ver al encontrar y publicar un nuevo fallo de seguridad.

Nuevamente, Google ha revelado públicamente una **nueva vulnerabilidad grave en Windows 7 y Windows 8.1** antes de que Microsoft haya sido capaz de desarrollar un parche, dejando a los usuarios de ambos sistemas operativos expuestos a los piratas informáticos hasta el próximo mes, cuando la compañía planea ofrecer una solución.

# Divulgación De Fallos sin parchear, bueno o malo?

Al parece la **política 90 días para la divulgación de fallos de seguridad de Google**, parece ser una buena medida para todos los proveedores de software para solucionar las fallas de seguridad antes de que sean explotados por los hackers y cibercriminales. Aunque esto al parecer no aplica a Microsoft, ya que en esta oportunidad se ha encontrado el **tercer fallo de seguridad**, a lo cual Google ha publicado inmediatamente el fallo y todo lo relacionado técnicamente con este problema. Sin duda los únicos afectados son los **usuarios que usan Windows 7 y Windows 8.1**.

La revelación de la falla de seguridad también fue parte del Proyecto Zero de Google, una iniciativa que identifica los agujeros de seguridad en diferentes programas y pide a las empresas que divulguen públicamente los parches de los bugs.

> *Chris Betz, director senior del Centro de Respuesta de Seguridad de Microsoft, escribió que el movimiento de Google «se siente menos como principios y más como un 'te pillé», y los clientes de Microsoft son los que sufren las consecuencias.» Y continúa: «Lo que es bueno para Google no siempre es lo adecuado para los clientes. Instamos a Google a hacer de la protección de los clientes el principal objetivo colectivo».*

Esta vez, el gigante de los buscadores ha descubierto un fallo en la función de memoria de cifrado CryptProtectMemory encontrado dentro de Windows 7 y 8,1 y se presenta tanto en las arquitecturas de 32 y 64 bits, esto puede revelar accidentalmente información sensible o permitir que un atacante pueda eludir los controles de seguridad.

# El Parche Del Fallo Llegará En Febrero Del 2015


Google primero notificó a Microsoft de la vulnerabilidad en Windows 7 y 8,1 el 17 de octubre de 2014. A continuación, Microsoft confirmó los problemas de seguridad el 29 de octubre y dijo que sus desarrolladores lograron igualar el agujero de seguridad. El parche para la vulnerabilidad está programada para el 10 de febrero.

La vulnerabilidad fue encontrada por **James Forshaw**, que también descubrió un «**defecto en el escalado de privilegios**» en Windows 8.1, se dio a conocer a principios de esta semana y atrajo fuertes críticas de Microsoft. El bug recién descubierto en realidad reside en la aplicación **CNG.sys**.

> *«El problema es la implementación en **CNG.sys** que no comprueba el nivel de suplantación de la pestaña al capturar el ID de inicio de sesión (utilizando SeQueryAuthenticationIdToken) por lo que un usuario normal puede suplantar a nivel de identificación y descifrar o cifrar los datos para esa sesión de inicio de sesión» James Forshaw dice en el post que revela la vulnerabilidad.*

Esta es la **tercera vez en menos de un mes** que el Proyecto Zero de Google dio a conocer detalles de la vulnerabilidad en el sistema operativo de Microsoft, después de sus 90 días divulgación pública política plazo. Hace unos días, **Google dio a conocer detalles de un nuevo error** de escalada de

privilegios en el sistema operativo Windows 8.1, el cual Microsoft planeaba solucionar, pero Google, no le dio plazo para no quedar mal ante los usuarios.