# Microsoft Soluciona Fallos De Stuxnet Y FREAK

Microsoft ha llegado con su más importante actualizacion para este año el martes, frente a la crítica del ataque de cifrado FREAK recientemente revelada, y una vulnerabilidad de cinco años de edad, separada aprovechado por el malware Stuxnet para infectar el sistema operativo Windows.

El malware Stuxnet, un sofisticado software malicioso de ciberespionaje supuestamente desarrollado por la Inteligencia de Estados Unidos y el gobierno israelí juntos, fue especialmente diseñado para sabotear las instalaciones nucleares iraníes hace algunos años. Fue descubierto en 2010, Stuxnet es dirigido a los equipos aprovechando vulnerabilidades en los sistemas Windows.

Afortunadamente, **Microsoft** ha publicado un parche para proteger sus equipos con Windows, los cuales son vulnerables a Stuxnet y otros ataques similares durante los últimos cinco años. La compañía también ha publicado una actualización que parchea la vulnerabilidad de cifrado FREAK, en su implementación SSL/TSL llamado canal seguro (**Schannel**). Las correcciones para la vulnerabilidad se incluyen en MS15-031.

Como hemos mencionado en nuestro informe anterior, **FREAK**, inicialmente se pensó para asociarse con el navegador Safari de Apple y los **navegadores de por defecto de Android**, pero se encontró que también puede afectar a los PC con Windows.


La **vulnerabilidad FREAK** permite a un atacante en la red para forzar el software utilizando componentes Schannel como Internet Explorer para utilizar el cifrado débil en la web, de modo que puedan descifrar fácilmente las conexiones HTTPS interceptadas.

Entre estos dos temas críticos, la compañía también ha lanzado un montón de otras actualizaciones el martes de marzo del 2015, en la cual se agrupa un total de 14 actualizaciones relacionadas con la seguridad para 43 vulnerabilidades que afectan a Internet Explorer, VBScript, Servicios de texto, Drivers Adobe Font, y Office.

- MS15-018 – Una actualización de seguridad acumulativa, calificado como «crítica», afecta a todas las versiones de **Internet Explorer** y aborda una serie de vulnerabilidades de corrupción de memoria, dos elevaciones de vulnerabilidades de privilegio, y una vulnerabilidad de corrupción de memoria VBScript.
- MS15-019 – Esta actualización soluciona una vulnerabilidad de secuencias de comandos en algunas versiones anteriores de los sistemas operativos Windows. La vulnerabilidad no afecta a Windows 7 y las versiones de escritorio posteriores.
- MS15-021 – Abarca ocho vulnerabilidades en los componentes del controlador Adobe Font para Windows y Windows Server explotables a través de un sitio web

malicioso o un archivo. También tiene una clasificación de «crítica» debido a la posibilidad de ejecutar código remoto.

- MS15-022 – Esta actualización corrige tres fallos desconocidos en formatos de documentos de oficina, así como cuestiones de cross-site scripting (XSS) múltiple para SharePoint Server, y se aplica a todas las versiones de Microsoft Office, así como los de Office Web Apps basadas en servidores y productos de SharePoint Server.
- MS15-023 – Este boletín, calificado como «importante», se ocupa de cuatro vulnerabilidades en el controlador de Windows en modo de núcleo que permite la elevación de los ataques de privilegio y de divulgación de información mediante el lanzamiento de una aplicación especialmente diseñada.

***Microsoft*** aconseja a todos sus usuarios y administradores instalar las nuevas actualizaciones tan pronto como sea posible.