Vulnerabilidades «Meltdown» y «Spectre» afectan a los servidores web

Las **Vulnerabilidades** «**Meltdown**» y «**Spectre**» afectan a los servidores web, no solo a las computadoras basadas en procesadores Intel y AMD. ¿Esto que quiere decir? ¿Que nuestros sitios web están expuestos a **exploits**? ¿Alguna solución a la vista?

En **HostDime**, preocupados por la integridad de la información de nuestras máquinas virtuales y servidores dedicados, trabajamos a marchas forzadas para **actualizar con los parches oficiales** el respectivo software en la medida que vaya saliendo. Esto quiere decir que es posible que debamos reiniciar los servidores de la compañía cuando esto suceda; se hará de forma gradual e inteligente. No hay razón para alarmarse pues todo está calculado milimétricamente para atenuar cualquier impacto.

Esta falencia encontrada hace pocos días por miembros de **Google Project Zero**, en dichos **procesadores**, permiten que procesos extraños y deshonestos lean la **memoria kernel**, es decir que atacantes remotos pudieran usar y explotar, para hacerse con contraseñas y datos de usuarios entre otras, así como cualquier información que otros programas , ejecutados en el mismo servidor. De todas formas, según manifiestan las compañías fabricantes de los procesadores, no hay pruebas de que esta falla haya sido explotada comercialmente por los hackers.

Los parches de Intel, se dicen que pueden ralentizar los procesadores en cifras que oscilan entre el 1 y el 14%. ¿Por

qué? Porque deben cortar los nexos entre la memoria kernel y los mismos, dando un rodeo por así decirlo. Estos valores dependen de la carga del chip parcheado. No resulta lo mismo de impactado un sistema con pocos procesos a uno que se mantiene al límite. Se dice por ejemplo que las instancias de Windows Server se verán afectadas si hay bastantes procesos E/S

Ya **existen parches para Linux y Windows**, así como para otros sistemas operativos. No obstante ha sido una semana ardua y convulsa para las empresas fabricantes de estos chips y el personal de los respectivos sistemas operativos perfeccionando los respectivos parches para tratar de mitigar los riesgos.

Se empieza la avalancha de demandas y procesos judiciales contra Intel porque se asegura que ellos conocían de esta vulnerabilidad hace varios meses y solo hasta ahora que se masificó la noticia, procedieron a tratar de contrarrestarla.

Ver también: Ataques DDoS en litespeed web server, cómo los maneja, Servidores web basados en procesos vs web server por eventos