Marcos González García - UO282587
Eduardo Blanco Bielsa – UO285176

Las migraciones por el año 2000. 296,7 billones de dólares

Enlace a la noticia

- Ver noticia

Resumen

El “Efecto 2000” también conocido como “Y2K” es un bug o un error de software que se temía que tuviese letales consecuencias y que trascendiese más allá del mundo de la informática a finales del siglo XX. Estaba basado en la idea de que, una vez diera comienzo el nuevo milenio, los ordenadores lo marcarían como año 00, retrocediendo, de este modo, hasta el 1900.

Razonamiento

Debido a que los equipos de la época eran especialmente complejos y había poca documentación sobre ellos, los ingenieros se dieron cuenta de que este bug podría afectar a muchísimas áreas profesionales, por lo que estaban realmente preocupados, ya que los sistemas fallarían por el uso de las fechas en aplicaciones informáticas. De esta forma, en el año 1999 prácticamente todo el mundo realizaba copias de seguridad masivas y comprobaciones sistemáticas sobre el “efecto 2000” para asegurarse de que realmente los sistemas podrían soportarlo.

Responsabilidad humana

La programación de los sistemas de aquella época fue ineficiente, y empresas como Microsoft e IBM tuvieron que dedicar mucho tiempo y recursos para poner solución al problema que habían introducido. Sus ingenieros tenían en sus manos un colapso global como nunca visto, pues servicios como bancos, supermercados y más establecimientos podrían dejar de funcionar por un tiempo indefinido.

Solución propuesta

Estas empresas aconsejaban realizar copias de seguridad periódicas, así como de revisar de forma pertinente que el sistema concreto podría soportar el Y2K. Ciertamente, no es la mejor solución, pues este problema debería haberse tenido en cuenta desde un principio para que no afectase directamente al cliente final (las personas que usasen los sistemas). Sin embargo, teniendo en cuenta la gravedad del fallo, fue la solución más rápida y económica por parte de los fabricantes de los sistemas informáticos de la época.

Marcos González García - UO282587
Eduardo Blanco Bielsa – UO285176

Intel ZombieLoad

Enlace a la noticia

- Ver la noticia

Resumen

Se ha descubierto una vulnerabilidad de los procesadores de Intel que permite a atacantes anular las protecciones del procesador y permite que aplicaciones en modo usuario accedan a datos procesados por la memoria en modo núcleo.

Razonamiento

El cómo hacen esto es explotando el hecho de que la cola del búfer de datos es accesible por todas las CPUs lógicas de un núcleo físico y no distingue entre procesos ni niveles de privilegio.

Responsabilidad humana

Esto es responsabilidad de los ingenieros de Intel, pues han dejado en los procesadores la cola del búfer de datos desprotegidos, sin comprobar la validez de quién está accediendo a ellos.

Solución propuesta

La solución sería modificar el búfer de forma que compruebe qué está accediendo a los datos y restringiéndolo sólo a componentes en los que el equipo pueda confiar.