

Vulnerabilidades en NTP(Hora de actualizarse?)

by javier - Domingo, octubre 25, 2015

<http://memoriasdeunsysadmin.info/vulnerabilidades-en-protocolo-ntp/>



Bases de NTP

NTP(Network Time Protocol) es el protocolo usado para sincronizar computadoras y demás dispositivos con "servidores oficiales de tiempo", a través de internet. Es un protocolo que ya lleva muchos años en uso y utiliza el puerto 123/UDP, de manera de poder hacer que actualice utilizando paquetes muy pequeños y s evitando adiciones de tráfico que en su momento eran innecesarias.

El precio de quedarse obsoleto

Ahora bien, como suele ocurrir en el campo de la tecnología, es solo cuestión de unos pocos años para que algo quede obsoleto y NTP no es la excepción. La falta de seguridad en la comunicación de un cliente con un servidor tiene una consecuencia muy grave: Permite ataques MITM(man-in-the-middle) de manera que un atacante puede pretender ser el servidor legítimo y alterar el reloj de todos los clientes que lo tengan en su camino.

Algunos Ejemplos:

Y cuál es el gran problema con que cambien el reloj de mi equipo, se preguntarán. Vamos a citar algunos, yendo de menor a mayor gravedad:

- Se sabe de numerosas aplicaciones que no funcionan correctamente si el reloj no tiene la hora correcto, para empezar, ya sea porque la licencia tiene un período definido de validez, o porque se base en la edad para permitir registros de usuarios nuevos(lo que se traduciría por ejemplo en imposibilidad de un usuario de registrarse) y un largo etcétera de formas en las que el código de miles de aplicaciones de todo tipo dependen del tiempo para algunas de sus funciones.
- Imposibilidad de acceder algunos sitios, debido a que el período de validez de su certificado es

posterior o anterior a la fecha y hora actuales. Esto puede depender del navegador que usemos y podría llegar a saltarse en navegadores viejos...

Efectos sobre HTTPS

- A la vez, un atacante podría aprovecharse del punto anterior. Un servidor(o cualquier equipo) podría aceptar certificados ilegítimos que ya fueron revocados tiempo atrás pero que pueden volver a ser válidos si el equipo ha vuelto al pasado. Un claro ejemplo es el caso de Heartbleed, una vulnerabilidad de muy alta serveridad que debió ser corregida revocando más de 100.000 certificados. Estos volverían a ser aceptados por cualquier equipo que recibiera una fecha anterior a mediados del 2014.
- Hay una gran cantidad de casos similares, agravado esto por el hecho de que una gran mayoría de navegadores aún hoy aceptan certificados de seguridad obsoleta, con lo cual, volver 5 o 10 años atrás implicaría aceptar conexiones usando certificados SSL fácilmente espiables y permitiendo al atacante monitorear todo nuestro tráfico a voluntad. Piensen ustedes mismos todo lo que puede verse espiando los datos que creemos se transmiten seguramente al navegar por internet o, peor aún, cuando un servidor se comunica con distintos servicios a través de internet.
- Salta a la luz, pero quiero darles un ejemplo claro en caso que alguno no lo haya imaginado: Supongamos que tengo una cuenta en el Banco X. Una vez por semana o cuando lo necesito, accedo tranquilamente a mi homebanking(supuestamente estoy bastante seguro, porque accedo a través de <https://bancox.com.ar>) que, de nuevo supuestamente, asegura a mi computadora que se está conectando al sitio legítimo del banco X. Qué pasa si alguien pone una notebook entre mi computadora y mi router(o bien dentro de la red de mi proveedor de internet), y monta un sitio con el dominio bancox.com.ar y con un certificado falso?. Este es un escenario muy particular pero no por ello difícil de lograr.

Más puntos débiles:

Otro factor que aumenta la debilidad de NTP es la dificultad de conseguir llaves para autenticar un servidor NTP. Los entes que las distribuyen son contados y los requisitos son muy exigentes.



Para el usuario no-informático, deben tener en cuenta que equipos viejos corriendo, por ejemplo, Windows XP, por defecto utilizan la hora del equipo, dependiendo de la pila de la BIOS(Esa famosa pila que hay que cambiar cada tanto). De ese modo NO usa servidores en internet, pero a cambio, si la pila se gasta, no hace falta ningún hack :D. Que sirva para darnos cuenta de lo importante de cambiar la bendita pila. Sistemas más nuevos en cambio, tienen la actualización de la hora automáticamente a través del servidor de NTP time.windows.com.

En el caso de empresas, no siempre es buena idea tal configuración, muchas veces es necesario asegurarnos de que todos los equipos tienen la misma hora(Uno de los motivos que impulsó la creación de NTP).

Atenuantes?

NTP tiene una protección nativa que puede ser de alguna ayuda(aunque no demasiada) contra estos ataques, El protocolo fue diseñado para prevenir cambios bruscos(de más de 16 minutos). Dicho límite es llamado umbral de pánico y, una vez alcanzado, el cliente rechazará la actualización y guardará un registro de error. Sin embargo hay maneras sencillas de saltarse esta protección: Una es simplemente, ir provocando cambios menores al umbral hasta llegar al efecto deseado. Otra manera implica reiniciar el equipo y disparar la actualización apenas haya reiniciado. Esto se basa en que el tiempo es reseteado(por defecto en algunos sistemas operativos en el reinicio por lo que aceptará cualquier valor inicial.

memoriasdeunsysadmin.tk