Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-001 Ataques de amplificación NTP utilizando CVE-2013-5211

Un ataque de amplificación del Protocolo de Tiempo de Red (NTP) es un tipo emergente de denegación de servicio distribuida (DDoS), que se basa en el uso de servidores NTP públicamente accesibles para saturar el sistema de la víctima con tráfico UDP.

- **Fecha de Liberación:** 1-Ene-2014
- **Ultima Revisión:** 22-Abr-2014
- **Fuente:** https://www.us-cert.gov/ncas/alerts/TA14-013A
- **CVE ID:** CVE-2013-5211
- **Riesgo** Moderado
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Negación de servicio

Sistemas Afectados

Servidores NTP < 4.2.7

1. ## Descripción

   El servicio NTP soporta un servicio de monitoreo que permite a los administradores consultar al servidor para obtener el conteo de clientes conectados. Esta información se proporciona a través del comando "monlist". La técnica básica de ataque consiste en que enviar una petición get monlist" a un servidor NTP vulnerable, que tiene como dirección de origen una falsificación de la dirección de la víctima.

2. ## Impacto

   El ataque se basa en la explotación de la característica 'monlist' de NTP, tal como se describe en CVE-2013-5211, que se encuentra habilitada de forma predeterminada en los dispositivos obsoletos con capacidad para NTP. Este comando crea una lista de las últimas 600 direcciones IP que se conectaron con el servidor NTP y la envía a la víctima. Dado que utiliza una dirección de origen falsificada, la respuesta del servidor NTP es enviada a la víctima. Puesto que el tamaño de la respuesta por lo general es considerablemente más grande que la solicitud, el atacante es capaz de amplificar el volumen del tráfico dirigido a la víctima. Además, debido a que las respuestas son datos legítimos procedentes de servidores válidos, es especialmente difícil bloquear este tipo de ataques. La solución es desactivar el comando "monlist" en el servidor NTP o actualizar a la última versión de NTP (4.2.7), que desactiva la funcionalidad "monlist".

3. ## Detección

   En una plataforma UNIX , el comando " ntpdc " consultará a los servidores NTP existentes sobre los datos monitoreados. Si el sistema es vulnerable a la explotación, responderá al comando "monlist" en modo interactivo. Por defecto, la mayoría de las distribuciones modernas de UNIX y Linux permiten que este comando sea utilizado desde localhost, pero no desde un host remoto. Para comprobar que existe soporte para el comando monlist, ejecute el siguiente comando:

/usr/sbin/ntpdc < servidor remoto >
monlist

Adicionalmente, el script "ntp-monlist" está disponible para NMap y mostrará automáticamente los resultados del comando monlist. Si el sistema no soporta la consulta monitor, y por lo tanto no es vulnerable a este tipo de ataque, NMap devolverá un error de tipo 4 (no hay datos disponibles) o ninguna respuesta en absoluto.

4. Solución

Como todas las versiones de ntpd antes de la 4.2.7 son vulnerables por defecto, la solución más simple recomendada es actualizar todas las versiones de ntpd que son de acceso público a, por lo menos, la versión 4.2.7. Sin embargo, en los casos en donde no sea posible actualizar la versión del servicio, se puede desactivar la funcionalidad de monitor en las versiones anteriores del software.

Para desactivar la función "monlist" en un servidor NTP disponible al público que no se puede actualizar a 4.2.7, añada la directiva "noquery" a la línea "restict default" (restringir por defecto) en el archivo del sistema ntp.conf, como se muestra a continuación:

restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

5. Referencias

o Vulnerability Summary for CVE-2013-5211
o NTP Software Downloads
o ntp-monlist NSE Script

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Lilia Elena Gonzalez Medina (lgonzalez at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47