Vulnerabilidad NTP Monitor

1. INTRODUCCIÓN

El servicio NTP (network time protocol) soporta un servicio de monitoreo que permite a los administradores consultar al servidor para obtener el conteo de clientes conectados. NTP se ejecuta a través del puerto UDP 123.

La técnica básica de esta vulnerabilidad consiste en enviar una petición “get monlist" a un servidor NTP vulnerable, que tiene como dirección de origen una falsificación de la dirección de la víctima.

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.

2. RIESGO

El ataque se basa en la explotación del comando 'monlist' de NTP, que se encuentra habilitado de forma predeterminada en servidores NTP anteriores a la versión 4.2.7. 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.

3. DETECCIÓN

Además de la debilidad intrínseca de UDP, que posibilita el efecto de reflexión falsificando la IP origen del paquete, existe una funcionalidad de monitorización de NTP que proporciona el efecto de amplificación de la respuesta. Esta funcionalidad está presente en servidores NTP con versión anterior a 4.2.7. Así, al hacer una consulta a un servidor no actualizado con el comando de monitorización *monlist* se consigue que éste

responda con la lista de las últimas máquinas con las cuales ha interaccionado (hasta 600). Obviamente, esta respuesta puede ser bastante grande en relación a la propia consulta.

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:

ntpdc -n -c monlist [ip]

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.

INFORMACIÓN DE LOS CAMPOS ADJUNTOS AL REPORTE:

Campo	Descripción
vulnerabilidad	Nombre de la vulnerabilidad reportada
direccion_ip	Dirección IP del dispositivo en cuestión
puerto	Puerto que responde a la vulnerabilidad
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
as_name	Nombre del ASN
status_EcuCERT	**Estado de la vulnerabilidad** **Online:** vulnerabilidad reportada por Feeds y comprobada por el EcuCERT en el timestamp_EcuCERT **Offline:** Vulnerabilidad reportada por Feeds, pero en el timestamp_EcuCERT no se detectó.
timestamp	Tiempo en la que la IP fue probada en UTC+0
ip	Dirección IP del dispositivo en cuestión
protocol	Protocolo que la respuesta NTP vino (UDP)
port	Puerto que la respuesta NTP vino
hostname	Nombre DNS inversa del dispositivo en cuestión
packets	Número total de paquetes que se reciben del dispositivo en cuestión

size	Cantidad total de datos (en bytes) recibidos del dispositivo en cuestión
asn	ASN en donde el dispositivo en cuestión se aloja
geo	País en donde el dispositivo en cuestión reside
region	Provincia
city	Ciudad en donde el dispositivo en cuestión reside

4. ACCIONES RECOMENDADAS

- Actualizar la versión del servidor NTP a 4.2.7p26 o superior, lo que resuelve el problema al quedar inhabilitado el comando monlist.
- Desactivar las consultas de monitorización, o restringir su acceso, en la configuración ntp.conf mediante el siguiente comando:

  disable monitor

- Como alternativa, si se pretende mantener la monitorización, puede restringirse su uso a redes internas:

  restrict default noquery
  restrict localhost
  restrict 192.168.0.0 netmask 255.255.0.0
  restrict 192.168.1.27

5. REFERENCIAS

- https://ipmiscan.shadowserver.org/
- http://unaaldia.hispasec.com/2017/03/multiples-vulnerabilidades-en-ntp.html.
- https://www.certsi.es/blog/ataques-dos-ntp
- https://ics-cert.us-cert.gov/advisories/ICSA-14-353-01C
- https://www.seguridad.unam.mx/historico/vulnerabilidadesDB/index.html-vulne=6491