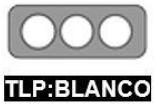

NTP Versión

(NTP: Network Time Protocol)

1. INTRODUCCIÓN

Este informe identifica servidores NTP que tienen el potencial de ser utilizados por delincuentes en ataques de amplificación para realizar ataques de denegación de servicio.

La técnica básica de este ataque consiste en enviar una petición con el comando “readvar" 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

NTP es un protocolo utilizado para sincronizar relojes entre sistemas informáticos en una red. Si bien NTP es muy útil, también se sabe que está plagado de varios defectos de seguridad, y a menudo se ha abusado de ellos para amplificar los ataques de denegación de servicio (DDoS) distribuidos. La última actualización de NTP, ntp-4.2.8p4, resuelve un total de 13 fallas, incluida la denegación de servicio (DoS).

UDP, es un protocolo no orientado a conexión que no valida las direcciones IP de origen, a menos que el protocolo de capa de aplicación utilice mecanismos de inicio de sesión. Cuando el paquete UDP tiene la dirección IP de origen falsificada (victima), el servidor responde a la víctima, creando un ataque de Denegación reflejada de servicio (RDoS).

El ataque se basa en la explotación del comando 'readvar' 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

Para comprobar manualmente si un sistema es vulnerable, puede utilizar el siguiente comando:

ntpq -c rv [ip]

FORMATO CAMPOS DEL 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 (UDP)
port	Puerto que la respuesta NTP vino
hostname	Nombre DNS inversa del dispositivo en cuestión
asn	ASN en donde el dispositivo en cuestión se aloja
geo	País en donde el dispositivo en cuestión reside
region	Estado / Provincia / Región Administrativa donde el dispositivo se encuentra
city	Ciudad en donde el dispositivo en cuestión reside
version	Versión de software NTP y el tiempo de creación
clk_wander	*“clock frequency wander (PPM)”*
clock	Fecha y hora
error	Error de frecuencia
frequency	Desplazamiento de frecuencia (PPM) en relación con reloj de hardware
jitter	Jitter del reloj
leap	Indicador de advertencia de salto (0-3)
mintc	Constante de tiempo mínimo (log2 s) (3-10)

noise	"fase blanca" ruido, aka jitter
offset	Desplazamiento combinados del servidor relativo a este host
peer	Un número de identificación de los pares en uso.
phase	Desplazamiento combinados del servidor relativo a este host
poll	Mensajes de poll enviados (por asociación con un reloj de referencia)
precision	Precisión (log2 s)
processor	Plataforma de hardware y la versión
refid	ID de referencia
reftime	Tiempo de referencia
rootdelay	Retardo de ida y vuelta total al reloj de referencia primaria
rootdispersion	Dispersión total al reloj de referencia primaria
stability	PPM desviación media frecuencia
state	El modo de operación actual NTP, donde 1 es simétrica activo, 2 es simétrica pasiva, 3 es cliente, 4 es el servidor, y 5 es de difusión.
stratum	El estrato del servidor del mismo nivel (1-15). Cualquier cosa mayor que 1 es una referencia secundaria
system	Sistema operativo y versión
tai	“TAI-UTC offest (s)”
tc	Constante de tiempo y exponente del poll (log2 s) (3-17)

4. ACCIONES RECOMENDADAS

- En el archivo de configuración del servidor NTP se debe incluir la siguiente línea:

  ntp-diasble-query-ntporg

- Actualizar la versión del servidor NTP. Todas las versiones del servidor NTP anteriores a 4.2.7 son vulnerables.

5. REFERENCIAS

- https://ipmiscan.shadowserver.org/
- http://es.galsys.co.uk/news/what-is-ntp-what-are-its-benefits-a-galleon-systems-guide/
- https://tools.ietf.org/html/rfc5905
- https://knowledgebase.uchicago.edu/page.php?id=37208&no_frill=1