Network Time Protocol (NTP) Mode 6 Scanner

Cosa sono le query in modalità 6 del servizio NTP, qual è il rischio e come è possibile mitigarlo? In attacchi informatici, supporto Che cos'è?

Network Time Protocol (NTP) viene utilizzato per sincronizzare l'orologio del computer con altri computer su Internet. Di gran lunga l'uso più comune di NTP è che un computer chieda "che ore sono?" di un altro computer. Ma NTP ha molte altre funzionalità, meno utilizzate. I comandi "Modalità 6" consentono di riconfigurare NTP mentre è in esecuzione.

Le richieste NTP possono essere utilizzate per organizzare un attacco Denial of Service, quando un utente malintenzionato tenta di sopraffare il server di una vittima inondandolo di richieste. In un attacco DDoS (Distributed Denial of Service), l'aggressore utilizza un esercito di server di terze parti inconsapevoli per attaccare la vittima contemporaneamente.

Perché è un rischio?

Poiché NTP viene utilizzato così frequentemente, utilizza l'efficientissimo User Datagram Protocol (UDP) per le comunicazioni. Uno dei motivi per cui UDP è così efficiente è che non esegue alcun tipo di “stretta di mano” quando riceve una richiesta.

Alcuni comandi della “Modalità 6” hanno la forma “Genera un rapporto e invialo a xxxxx”. È possibile sferrare un attacco DDoS contro una vittima inviando richieste a MOLTI server NTP, formando una “bot-net”, sostituendo xxxxx con l’indirizzo di rete della vittima. Il conseguente flusso di segnalazioni può sovraccaricare il computer della vittima. Un DDoS è particolarmente efficace se la dimensione del report generato è maggiore della dimensione del comando che produce il report.

Come puoi mitigare il rischio?

Mitigare questo rischio è difficile perché la vittima non è realmente parte del problema.

Il modo migliore per mitigarlo (e questo vale per tutti i rischi di attacco DDoS) è assicurarsi che i tuoi computer non possano essere indotti con l’inganno a diventare parte di una “bot-net”.

Puoi:

Interrompi la fornitura di servizi NTP su Internet bloccando il traffico NTP con il firewall. Utilizzare invece un Time Server pubblico. Aggiorna all'ultima versione del server NTP e proteggilo; ntp.org ha risorse per aiutarti. Utilizza una VPN per controllare gli utenti e i computer che possono accedere al tuo server. Utilizzare un server NTP interno: può essere costoso.

Risorse:

Attacchi DDoS NTP
https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

Manutentori ufficiali dell'NTP
http://www.ntp.org/

Output

- Nessus elicited the following response from the remote host by sending an NTP mode 6 query :

```
'version="ntpd 4.2.8p17@1.4004-o Wed Nov 29 06:04:45 UTC 2023 (1)",
processor="amd64", system="FreeBSD/14.0-CURRENT", leap=3, stratum=2,
precision=-24, rootdelay=42.383, rootdisp=183.276, refid=85.199.214.99,
reftime=0xea4b7c33.977f633d, clock=0xea4b7e2e.7db4bc55, peer=55921,
tc=6, mintc=3, offset=0.000000, frequency=61.578, sys_jitter=82.173085,
clk_jitter=0.000, clk_wander=0.609'
```

SSL Certificate Cannot Be Trusted

Descrizione:

Il certificato X.509 del server non può essere considerato attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena di fiducia può essere interrotta, come indicato di seguito:

- Innanzitutto, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica conosciuta. Ciò può verificarsi quando la parte superiore della catena è un certificato autofirmato non riconosciuto o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.

- In secondo luogo, la catena di certificati potrebbe contenere un certificato non valido al momento della scansione. Ciò può verificarsi quando la scansione avviene prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato.

- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrisponde alle informazioni del certificato o che non può essere verificata. Le firme errate possono essere risolte facendo sì che il certificato con la firma errata venga firmato nuovamente dall'emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato di un algoritmo di firma che Nessus non supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe rendere più semplice l’esecuzione di attacchi man-in-the-middle contro l’host remoto.

Soluzione

Acquista o genera un certificato SSL adeguato per questo servizio.

In crittografia, X.509 è uno standard dell'Unione internazionale delle telecomunicazioni (ITU) che definisce il formato dei certificati a chiave pubblica.[1] I certificati X.509 sono utilizzati in molti protocolli Internet, incluso TLS/SSL, che costituisce la base di HTTPS,[2] il protocollo sicuro per la navigazione sul web. Vengono utilizzati anche in applicazioni offline, come le firme elettroniche.[3]

Output

- The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

  |-Subject : O=pfSense GUI default Self-Signed Certificate/CN=pfSense-668e32e36adb1
  |-Issuer : O=pfSense GUI default Self-Signed Certificate/CN=pfSense-668e32e36adb1