راهنمای مشکل امنیتی

موجود بر روی NTP

راهنمای مشکل امنیتی موجود بر روی NTP

تاریخ تنظیم : مرداد ۱۳۹۸

گروه شرکت‌های شاتل

فهرست مطالب

NTP چیست؟

NTP یا پروتکل زمان تحت شبکه یکی از قدیمی‌ترین پروتکل‌های مورد استفاده در شبکه‌های مبتنی بر IP است که در سال ۱۹۸۵ توسط David L. Mills در دانشگاه Delaware طراحی و ایجاد شد و در حال حاضر نسخه‌ای که مورد استفاده قرار دارد NTPv4 می باشد.

با استفاده از این پروتکل امکان هماهنگ نمودن و استفاده از ساعت دقیق در حد ساعت اتمی در شبکه های کامپیوتری بوجود می آید. معمولا در شبکه یا هر سیستم متصل به شبکه جهانی با اتصال به یک تایم سرور امکان تنظیم دقیق ساعت آن سیستم یا سیستم‌های آن شبکه بوجود می آید.

NTP از ساعت هماهنگ جهانی یا Coordinated Universal Time (UTC) که یک استاندارد زمان از نوع اتمی است برای هماهنگی ساعت کامپیوتر ها در حد میلی ثانیه استفاده می‌کند.

آسیب‌پذیری‌های پروتکل NTP

حملات NTP یکی از بزرگترین حملات DDOS از سال ۲۰۱۴ تا به امروز بوده است و حال بعد از گذشت ۵ سال هنوز سرورهای NTP آسیب پذیر زیادی در دنیا وجود دارد که به عنوان تقویت کننده برای Attackهای مربوط به NTP استفاده می‌شود.

پیاده‌سازی‌های پروتکل NTP در سالهای اخیر دارای آسیب پذیری کمتری شده است به این دلیل که دستور Monlist به صورت پیش فرض غیرقابل استفاده شده است. با این حال NTP های قدیمی و یا تغییراتی که بر روی NTP های جدید ایجاد شده است باز هم می تواند این پروتکل را به پروتکل ناامنی تبدیل کند.

راهکارهای کاهش آسیب‌پذیری از طریق پروتکل NTP

برای اینکه آسیب پذیری از طریق پروتکل NTP را کاهش دهید می توانید از راهکارهای زیر استفاده بفرمایید:

۱. ابتدا لزوم استفاده از این سرویس را بررسی بفرمایید . در صورتی که لزومی نمی بینید این سرویس را غیرفعال کنید.

۲. پورت ۱۲۳ را بر روی Interface مربوط به اینترنت خود محدود کنید و ببندید.

۳. بر روی فایروال شبکه خود درخواست های ناخواسته را مسدود کنید.

۴. سرور NTP خود را با نرم افزار های مربوط به یافتن آسیب پذیری‌ها اسکن کنید.

۵. NTP Daemon را به آخرین ورژن به روز رسانی فرمایید.

۶. اگر امکان ارتقا برای شما وجود ندارد دستور Monlist را غیرفعال کنید و یا درخواست های دریافتی را به Source IP مشخص محدود کنید.