باسمه‌تعالی

حملات DDoS با سوءاستفاده از سرویس تحلیل سرور MS-SQL

(MS-SQL Server Resolution)

شرح حمله

سرویس تحلیل سرور MS-SQL[1] این امکان را در اختیار کلاینت قرار می‌دهد که بتواند از نصب بودن SQL-Server بر روی سرور اطلاع پیدا کرده و جزئیات مربوط به SQL-Server نصب شده را دریافت کند. برای دریافت این اطلاعات، کلاینت یک درخواست یک بایتی به سوی سرور ارسال می‌کند و سرور در پاسخ یک پیام با طول متغیر شامل نام، نسخه و اطلاعات مربوط به اتصالات شبکه باز می‌گرداند.

در واقع کلاینت‌ها قبل از برقرای اتصال با SQL Server نیاز به دریافت اطلاعاتی از آن دارند که توسط این سرویس می‌توانند به اطلاعات مورد نظر دست پیدا کنند. تمامی نسخه‌های SQL Server از نسخه ۲۰۰۰ به بعد دارای این سرویس می‌باشند.

ویژگی‌های فوق سبب شده است تا این سرویس دارای شرایط لازم جهت اجرای حملات Reflected DDoS بوده و بتواند مورد سوء استفاده قرار گیرد (تولید و ارسال چندین بایت پاسخ به ازای هر بایت پرسش).

برای اجرای حمله، فرد حمله‌کننده درخواست تحلیل سرور MS-SQL را برای سرویس‌دهنده MS-SQL ارسال نموده ولی به‌جای قرار دادن آدرس IP خود در فیلد آدرس IP فرستنده، آدرس IP فرد قربانی را قرار می‌دهد. درنتیجه پاسخ تولیدی برای فرد قربانی ارسال خواهد شد. به دلیل اینکه تعداد بایت موجود در پیامی که سرور در پاسخ باز می‌گرداند نسبت به تعداد بایت موجود در پرسش ارسال شده از سوی کلاینت قابل توجه است، حمله‌کننده می‌تواند به ضریب تقویت[2] بالایی دست پیدا کند. بدین صورت با به‌کارگیری یک شبکه باتنت می‌توان حجم بسیار زیادی ترافیک به سوی فرد قربانی هدایت نمود. درنتیجه یک سرویس‌دهنده MS-SQL که پیکربندی صحیحی ندارد می‌تواند به‌طور ناخواسته در حمله DDoS مورد سوءاستفاده قرار گیرد.

این روش در اواخر سال ۲۰۱۴ میلادی و در پی حمله DDoS به یکی از شهرهای کشور آمریکا شناسایی شده است. در این حمله متوسط طول پاسخ بازگردانده شده از سمت سرور ۴۴۰ بایت بوده و با فرض اینکه طول بسته

[1] MS SQL Server Resolution Service (MC-SQLR)
[2] Amplification factor

درخواست ارسال شده به سمت سرور یک بایت باشد، بنابراین حمله کننده می‌تواند به ضریب تقویت قابل توجه ۴۴۰ دست پیدا کند (در صورت در نظر گرفتن تعداد بایت‌های سرایند، ضریب تقویت برابر ۲۲ خواهد بود).

روش امن‌سازی

بهترین روش جلوگیری از سوءاستفاده از این آسیب‌پذیری آن است که ابتدا صاحبان سرویس‌دهنده MS-SQL از نیازمندی قابل دسترس بودن این سرویس از طریق اینترنت اطمینان حاصل نمایند. در بسیاری از موارد، دلیلی برای وجود چنین دسترسی وجود ندارد. اما در صورت نیاز وجود دسترسی به MS-SQL از طریق اینترنت بایستی فضای آدرس مجاز به دسترسی به آن را محدود ساخت.

از سوی دیگر، سرویس تحلیل سرور MS-SQL تنها در صورتی نیاز است که چندین instance دیتابیس وجود داشته باشد. در بقیه موارد می‌توان این سرویس را غیرفعال نمود. از نسخه ۲۰۰۸ به بعد، این ویژگی به‌صورت پیش فرض غیرفعال بوده ولی همچنان در نسخه‌های Desktop Engine فعال است.

همچنین پروتکل MC-SQLR (Microsoft SQL Server Resolution Protocol) از پورت 1434/UDP استفاده می‌نماید. از این‌رو می‌توان با استفاده از دیواره آتش، ترافیک ورودی و خروجی از این پورت را کنترل نمود و آن را محدود به چندین آدرس نمود.

ضمناً می‌توان با افزودن یک لایه امنیتی بیشتر همچون احراز اصالت از طریق SSH یا VPN، جلوی سوءاستفاده از این آسیب‌پذیری را گرفت.