باسمه تعالی

آسیب‌پذیری عدم احراز هویت در Redis

فهرست مطالب

۱ مقدمه

Redis یک انبار ساختار داده داخل حافظه و متن باز (تحت لیسانس BSD) است که به عنوان پایگاه داده، حافظه کش و واسطه پیام استفاده می‌شود و از ساختمان داده‌هایی مانند رشته‌ها، هش‌ها، لیست‌ها، مجموعه-ها و مجموعه‌های مرتب شده با دامنه وسیعی از پرس‌وجوها و بیت مپ‌ها و شاخص‌های مکانی با مجموعه‌ای از پرس‌وجوها پشتیبانی می‌کند.

۲ آسیب‌پذیری عدم احراز هویت در Redis

Redis جهت دسترسی کلاینت‌های قابل اعتماد درون محیط‌های قابل اعتماد طراحی شده است که به این معناست که قرار دادن مستقیم نمونه‌ای از Redis در معرض اینترنت یا به طور کلی در معرض محیطی که در آن کلاینت‌های غیرقابل اعتماد می‌توانند مستقیماً به پورت TCP یا سوکت یونیکس Redis دسترسی داشته باشند ایده خوبی نیست. از آنجایی که این سرویس از احراز هویت پشتیبانی نمی‌کند، هر موجودیتی که بتواند به نمونه‌ای از Redis دسترسی داشته باشد می‌تواند بر روی انبار کلید-مقدار کنترل کامل داشته باشد.

به طور پیش‌فرض Redis تمام آدرس‌های IP که به پورت سرور redis (6379) دسترسی دارند را بدون هیچ احراز هویتی می‌پذیرد. مهاجم از راه دور قادر به استفاده از دستور "redis-cli -h [IP]"، و پس از آن "info" جهت کسب اطلاع از نسخه سرور Redis است. این دسترسی می‌تواند برای به دست آوردن کنترل کامل یک سرور Redis و محتوایی که ذخیره کرده است، استفاده شود.

۳ محصولات تحت‌تأثیر آسیب پذیری

تمام نسخه‌های Redis

۴ اقدامات جهت مقابله با آسیب‌پذیری

گزینه‌های مختلفی جهت محافظت از سرور یا دستگاه شما در دسترس است:

- اگر از Redis استفاده نمی‌کنید آن را غیرفعال کنید که آسان‌ترین و مؤثرترین راه‌حل است.
- قابلیت احراز هویت را در redis.conf پیاده سازی کنید.
- از دیوارآتش جهت مسدود کردن تمام اتصالات به پورت 6379، به جز از IP های قابل اعتماد استفاده کنید.
- یک کلمه عبور به پیکربندی خود اضافه کنید.

- اگر مجبور به اجرای redis در یک ناحیه غیرقابل اعتماد هستید، امنیت را در لایه-IP (به طور مثال با ipsec) فراهم کنید.
- مطمئن شوید پورتی که Redis برای گوش دادن جهت اتصالات استفاده می‌کند(به طور پیش‌فرض 6379 و علاوه براین اگر Redis را در حالت cluster اجرا کنید پورت 16379، و 26379 برای Sentinel) پشت دیوارآتش قرار دارد، بنابراین اتصال به Redis از دنیای بیرون ممکن نخواهد بود.
- اگر شما تنها به صورت محلی از همان کامپیوتر به Redis دسترسی دارید، تنها رابط loopback را برای redis فعال کنید.
- از گزینه requirepass به منظور افزودن یک لایه امنیتی اضافی استفاده کنید. بنابراین کاربران نیاز به احراز هویت با استفاده از دستور AUTH خواهند داشت.
- اگر محیط شما نیاز به رمزگذاری دارد از spiped یا دیگر نرم افزارهای تونلینگ SSL به منظور رمزگذاری ترافیک بین سرورها و کاربران Redis استفاده کنید.

در حالی که Redis سعی در پیاده سازی کنترل دسترسی ندارد، یک لایه کوچک احراز هویت که به صورت ویرایش اختیاری فایل redis.conf در آمده است ارائه می‌دهد.

هنگامی که لایه احراز هویت فعال باشد، Redis هر پرس‌وجو توسط کاربران غیرمجاز را رد خواهد کرد. یک مشتری می‌تواند با ارسال دستور AUTH و کلمه عبور احراز هویت کند. کلمه عبور توسط مدیر سیستم در داخل متن فایل redis.conf تنظیم می‌شود. این کلمه عبور باید جهت جلوگیری از حملات brute force به اندازه کافی طولانی باشد.

لازم به ذکر است دستور AUTH همانند دیگر دستورات Redis بدون رمزگذاری ارسال می‌شود، بنابراین کلمه عبور در برابر مهاجمی که دسترسی کافی به شبکه جهت اجرای استراق سمع دارد، محافظت نمی‌شود.