تحلیل آسیب پذیری پروتکل NAT-PMP و ارائه راهکارهای رفع آسیب پذیری

به تازگی مشخص شده است که بسیاری از دستگاه ها با قابلیتNAT-PMP به درستی پیکربندی نشده اند که موجب می شود تا درخواست های زیادی روی اینترفیس های شبکه خارجی دریافت گردد و یا map forwardingبه آدرس های دیگر از میزبان درخواست شده صورت گیرد. به این ترتیب آنها به طور بالقوه برای افشای اطلاعات و درخواست های port mappingمخرب آسیب پذیر خواهند بود.

شرح آسیب پذیری

NAT-PMPیک پروتکل مورد استفاده در روترها است که به برنامه های مورد استفاده کاربر داخلی اجازه می دهد بصورت خودکار دسترسی به منابع شبکه پشت NAT را از بیرون شبکه فعال نمایند. (در واقع عملکردی مشابه port forwarding بر روی دستگاه NAT کننده بدون دخالت کاربر صورت بگیرد).

مطابق RFC6886 [۳] gateway"NAT نباید درخواست های mapping با مقصد آدرس IP خارجیNAT gateway یا دریافت شده از اینترفیس شبکه خارجی اش را قبول نماید". علاوه بر این درخواست های mapping باید روی آدرس NAT شده داخلی نگاشته شود. هنگامی که یک NAT-PMP نتواند تا این محدودیت ها و پیکربندی نادرست را اجرا کند، ممکن است درخواست های port mapping آلوده را قبول یا اطلاعات خودش را افشا نماید.

طبق استاندارد درخواست های NAT-PMP تنها از مبدا IPهای داخلی شبکه (پشت NAT)باید پذیرفته شوند و درخواست های واصله به واسطه IP های خارجی یا valid قابل پذیرش نیست. این در حالی است درطول تحقیقات،حدود ۱.۲ میلیون دستگاه در اینترنت عمومی به پروبهای خارجیNAT-PMPپاسخ دادند. پاسخ های آن ها نشان دهنده دو نوع آسیب پذیری است؛ به کار بردن port mapping آلوده و افشای اطلاعات دستگاهNAT-PMP. که می تواند به ۵ صورت ذیل باشد:

- شنود ترافیک NATشبکه داخلی: ~ ۳۰۰۰۰ عدد دستگاه (۲.۵٪ازدستگاه های پاسخ دهنده)
- شنودترافیک خارجی: ~ ۱.۰۳ میلیون(۸۶٪ازدستگاه های پاسخ دهنده)
- دسترسی به سرویس های کاربرانNATداخلی: ~۱.۰۶میلیون(۸۸٪ازدستگاه های پاسخ دهنده)
- حمله DoSبه سرویس های میزبان: ~۱.۰۶ میلیون (۸۸٪ازدستگاههاپاسخ)
- استخراج اطلاعات دستگاه ~ NAT-PMP :۱.۲میلیون(۱۰۰٪دستگاه های پاسخ دهنده)

یک مهاجم از راه دور و بدون احراز هویت های لازم ممکن است قادر به جمع آوری اطلاعات درباره تجهیزات NAT، تغییر در Port mapping، شنود ترافیک خصوصی و عمومی، دسترسی به سرویس های خصوصی کاربر و بلوکه کردن سرویس های میزبان گردد.

راه حل ها

۱. پیکربندی امن NAT-PMP:
   - اینترفیس های LAN و WAN بدرستی اختصاص داده شود
   - درخواست های NAT-PMP فقط رو اینترفیس های اینترنت قبول شوند.
   - Port mapping فقط برای آدرس های IP داخلی درخواست کننده باز باشد.
۲. به روزرسانی miniupnpd: اگرچه آسیب پذیری های NAT-PMP به علت نقص در کد miniupnpd نیست، ولی بروزرسانی منتشر شده در آن قطعاً RFC 6886 را اجرا خواهد کرد. مطابق نسخه ۱.۸.۲۰۱۴۱۰۲۲، miniupnpd از بسته های NAT-PMP دریافت شده روی اینترفیس WAN صرف نظر می کند. فایل پیکربندی پیش فرض ارائه شده، miniupnpd.conf،در حال حاضر دارای تنظیمات بیشتری جهت افزایش امنیت پیکربندی است.
۳. محدود کردن دسترسی : اعمال رول های فایروال برای بلوکه کردن میزبان های غیرقابل اعتماد برای دسترسی به پورت 5351/udp.
۴. غیرفعال کردن NAT-PMP: غیرفعال سازی NAT-PMP روی دستگاه در صورتی که کاملاً غیرضروری باشد.

اطلاعات مربوط به فروشندگان

Vendor	Status	Date Notified	Date Updated
Grandstream	Affected	23 Sep 2014	28 Oct 2014
Netgear, Inc.	Affected	08 Oct 2014	28 Oct 2014
Radinet	Affected	23 Sep 2014	28 Oct 2014
Speedifi	Affected	23 Sep 2014	28 Oct 2014
Technicolor	Affected	16 Oct 2014	28 Oct 2014
Tenda	Affected	23 Sep 2014	28 Oct 2014
Ubiquiti Networks	Affected	08 Oct 2014	28 Oct 2014
ZTE Corporation	Affected	23 Oct 2014	28 Oct 2014
ZyXEL	Affected	08 Oct 2014	28 Oct 2014
Apple Inc.	Not Affected	10 Oct 2014	21 Oct 2014
MikroTik	Not Affected	23 Sep 2014	27 Oct 2014