Security Flaws in IPv6

Arash TaherKalateh 882980

کم کم با اتمام آدرس‌های موجود برای IP نسخه چهار، حرکت به سمت استفاده از IPV6 آغاز شده است. این قابلیت در اکثر سیستم عامل‌ها و دستگاه‌های تحت شبکه عمل شده است و تحقیقات در مورد امنیت ساختار آن توسط محققین آغاز شده است. با وجود محدوده گسترده آدرس‌دهی در IPV6 می‌توان گفت که هدف در آن ایجاد ارتباط End-to-End و یا Peer-to-Peer است. علاوه بر اینها در این نسخه با حذف و تعدیل Header های بسته امکان روت کردن آن نیز ساده تر شده است که آن را تبدیل به ابزاری ایده‌آل برای برنامه‌های VoIP و IM می‌کند.

با وجود تمام این مزایا اما، محققین اذعان به وجود نقص‌های امنیتی بعضا خطرناک در IPV6 کرده‌اند. به عنوان نمونه می‌توان اشاره کرد به مشکل امنیتی خطرناکی که اخیرا توسط گروهی فرانسوی کشف شده. طی این فرآیند می‌توان مقادیر متنابهی داده به سربرگ IPV6 اضافه کرد که روترهای تحت این پروتکل مجبور به پردازش آنها هستند. این تمام چیزی است که یک مهاجم در حمل DoS میتواند طلب کند. البته این مشکل در پیش‌نویس امنیتی IPV6 هم ذکر شده است و IETF به دنبال راه حلی برای اصلاح این روزنه (Routing type 0) میگردد.

از جمله مشکلات امنیتی دیگر در IPV6 (که به گفته Ivan Arce, CTO of Core Security Technologies ناشی از بپیچید بودن این پروتکل است) می‌توان به مورد زیر اشاره کرد :

Trespassing : قابلیت Advanced network discovery به شما این امکان را میدهد که مسیر حرکت بسته خود را مشخص کنید. مشکل اینجاست که این موضوع به مهاجم اجازه میدهد به قسمت‌های از شبکه و تجهیزاتی دسترسی پیدا کند که قرار بوده مخفی بماند.

Filtering device bypass : تجهیزات فعلی موجود برای تامین امنیت و فیلتر کردن شبکه، همچون Firewall و DMZ برای کار با IPV6 طراحی نشده‌اند. همچنین متخصصان نگرانند از اینکه بتوان این موانع را با Route Header 0 بتوان دور زد.

DoS (Denial-of-service) : می‌توان یک بسته را به نحوی تنظیم کرد که در یک حلقه بزرگ از Routing دائماً در چرخش باشد تا پهنای باندی بسیار بیش از آنچه نیاز دارد مصرف کند. تا این حد که به فردی به پهنای بند ۱.۵ Mbit اجازه میدهد لینکی با ظرفیت 100Mbit را Kill کند.

Anycast: Not safe anymore : این تکنیک به این صورت کار می‌کند که با اعلام کردن یک IP یکسان برای چندین نقطه اجازه میدهد شبکه تصمیم بگیرد روت کردن از کدام راه سریع‌تر و مطمئن تر است . مشکل در اینجا

هم باز از RH0 ناشی میشود، به این صورت که یکی از این بسته‌ها میتواند اعتبار سایر بسته‌ها را نقض کند. (در کلّ گفت شده که RH0 چیزی جز اینجا مشکلات عدیده امنیتی به همراه نداشته و بهتر از از IPV6 Protoocol به کلّ حذف شود.

مشکل‌سازی IPV6 برای IPV4 : یکی دیگر از مشکلات عمده دیگر این است که با باز کردن IPV6 ، ممکن است شما IPV4 و سایر تجهیزات شبکه خود را که پیش از این به درسته کار میکردند، در معرض خطرات و آسیب‌پذیری‌های از سمت IPV6 قرار دهید. این مشکل در حدی که بسیاری از شرکت‌ها حاضر نیستند IPV4 خود را، که از آن سوددهی دارند، این گونه در ریسک قرار دهند.