بسمه‌تعالی

بررسی آسیب‌پذیری دور زدن VPN

گزارش آسیب‌پذیری

در این گزارش به بررسی آسیب‌پذیری امنیتی دور زدن VPN در سیستم‌عامل iOS نسخه ۱۳.۴ که مانع از رمزنگاری کلیه ترافیک توسط VPN می‌شود، می‌پردازیم.

۱ آسیب‌پذیری دور زدن VPN در iOS چگونه کار می‌کند؟

عموماً پس از اتصال به یک شبکه خصوصی مجازی (VPN)، سیستم‌عامل کلیه اتصالات اینترنت موجود را قطع کرده و سپس آنها را از طریق تونل VPN مجدداً برقرار می‌کند.

اخیرا گروه Proton کشف کرده است که در سیستم‌عامل iOS نسخه ۱۳.۳.۱، کلیه اتصالات موجود قطع نمی‌شود (این آسیب‌پذیری در نسخه ۱۳.۴ نیز همچنان وجود دارد). بیشتر اتصالات کوتاه‌مدت بوده و مجدداً به تنهایی از طریق تونل VPN برقرار می‌شوند. با این حال بعضی از آنها بلندمدت بوده و می‌توانند تا دقایق و یا ساعاتی خارج از تونل VPN باز بمانند.

نمونه بارز آن، سرویس ارسال اعلان[۱] در Apple است که حاوی اتصالات بلندمدت بین دستگاه و سرورهای اپل می‌باشد. اما این مشکل می‌تواند روی هر برنامه یا سرویسی مانند برنامه‌های پیام‌رسانی سریع یا beaconهای وب[۲] تاثیر بگذارد.

در صورت عدم رمزنگاری اتصالات آسیب‌دیده، آسیب‌پذیری دور زدن VPN سبب افشای داده‌های کاربران خواهد شد. مشکل شایع‌تر نشت IP است. مهاجم می‌تواند آدرس IP کاربران و آدرس IP سرورهایی که به آن متصل می‌شوند را مشاهده کند. به‌علاوه، سروری که به آن متصل می‌شوید بجای آدرس VPN IP، آدرس واقعی شما را مشاهده می‌کند.

افراد در کشورهایی که نظارت و نقض حقوق شهروندی رایج است، بیشتر در معرض خطر این نقص امنیتی قرار دارند. هیچکدام از سرویس‌های ProtonVPN یا سایر VPNها نمی‌تواند راه‌حلی برای این مشکل پیدا کند؛ به این دلیل که سیستم‌عامل iOS به یک برنامه VPN اجازه نمی‌دهد اتصالات شبکه موجود را از بین ببرد.

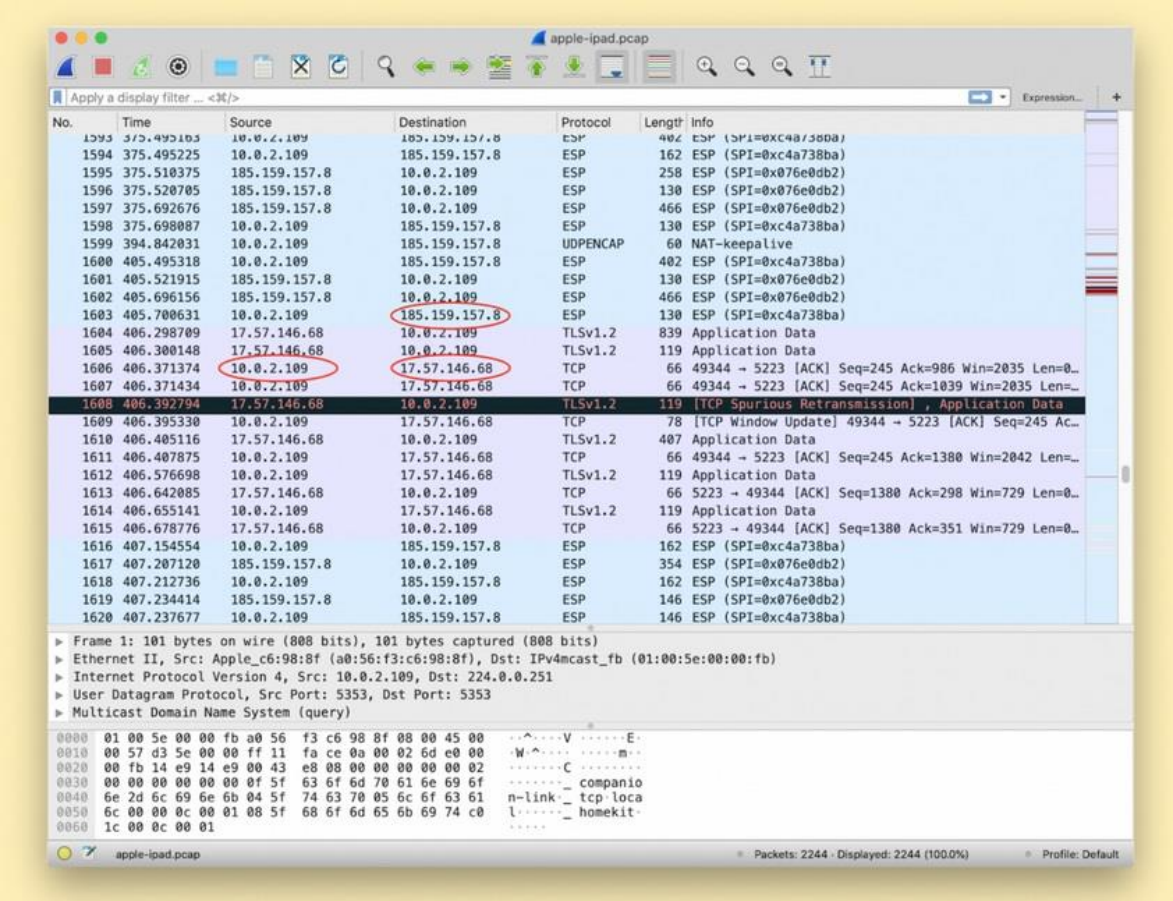
---

[۱] push notification

[۲] تکنیکی که در صفحات وب و ایمیل استفاده می‌شود تا به نحوی که برای کاربر مشهود نیست، دسترسی کاربر به بعضی محتواهای سایت را بررسی کند.

۲ بررسی آسیب‌پذیری

هنگامی که دستگاه به VPN متصل می‌شود، فقط می‌توان ترافیک بین IP دستگاه و سرور VPN یا آدرس‌های IP محلی (دستگاه‌های دیگر در شبکه) را مشاهده کرد. همان طور که شکل زیر مشاهده می‌شود یک ترافیک مستقیم بین IP دستگاه iOS و آدرس IP خارجی (که سرور VPN نیست) نیز وجود دارد (در این مثال یک سرور Apple است).



شکل ۱ : capture کردن ترافیک دستگاه iOS با نرم‌افزار Wireshark

آدرس IP دستگاه iOS: 10.0.2.109

سرور ProtonVPN: 185.159.157.8

آدرس IP متعلق به Apple: 17.57.146.68

شدت این آسیب‌پذیری متوسط محاسبه شده است.

۳ کاهش مخاطرات آسیب‌پذیری دور زدن VPN در iOS

اتصالات اینترنتی که پس از اتصال به VPN برقرار می‌شوند تحت تاثیر این آسیب‌پذیری قرار نمی‌گیرند. اما اتصالاتی که هنگام اتصال به VPN در حال اجرا هستند، ممکن است برای یک مدت نامحدود در خارج از تونل VPN برقرار بمانند و هیچ تضمینی برای اینکه اتصالات در لحظه ایجاد اتصال VPN قطع شوند، وجود ندارد.

با این حال، روش زیر تقریباً به همان اندازه موثر است:

۱) اتصال به هر سرور VPN
۲) فعال کردن حالت هواپیما. این کار کلیه اتصالات اینترنت را قطع کرده و موقتاً VPN را غیرفعال می‌کند.
۳) غیرفعال کردن حالت هواپیما. VPN مجدداً متصل شده و اتصالات دیگر مجدداً در تونل VPN برقرار می‌شوند. اگرچه نمی‌توان این مسئله را صددرصد تضمین کرد.

از طرف دیگر، اپل برای کاهش این مخاطرات این آسیب‌پذیری استفاده از Always-on VPN را توصیه می‌کند. این روش به استفاده از تنظیمات مدیریت دستگاه در محصولات اپل نیاز دارد، بنابراین متأسفانه آسیب‌پذیری برنامه‌های شخص ثالث مانند ProtonVPN را برطرف نمی‌کند.

این آسیب‌پذیری برای نخستین بار توسط Luis، مشاور امنیتی و عضو جامعه Proton گزارش شد. شرکت اپل آسیب‌پذیری دور زدن VPNرا تایید کرده و به دنبال روش‌هایی برای کاهش آن است. تا زمانی که به‌روزرسانی جدیدی برای اپل منتشر نشود، استفاده از راه‌حل‌های فوق توصیه می‌شود.

۴ مراجع

[1] https://protonvpn.com/blog/apple-ios-vulnerability-disclosure/