بعد از گذشت پنج ماه از شناسایی رخنه HTTPS

برنامه‌های آندروید همچنان بی‌دفاع

بیش از هفت ماه از شناسایی آسیب‌پذیری مهمی که توسط محققان کالج City در سان‌فرانسیسکو کشف شد، می‌گذرد. بیش‌تر از یک دوجین برنامه آندروید که حداقل 350 میلیون بار دانلود شده‌اند، هنوز هم حاوی رخنه‌ای در پروتکل HTTPS هستند که باعث می‌شود گذرواژه‌ها، شماره تلفن‌ها و دیگر داده‌های حساس و مهم کاربر به بیرون درز پیدا کنند.

این برنامه‌های آسیب‌پذیر عبارت‌اند از:
OKCupid Dating, Dish Anywhere, ASTRO File Manager with Cloud, CityShop-for Craigslist, PicsArt Photo Studio.

با توجه به آمارهای به‌دست آمده از Google Play، این برنامه‌ها در مجموع 170 میلیون تا 670 میلیون بار دانلود شده‌اند. سام بان محقق امنیتی دانشگاه City سان‌فرانسیسکو که درباره هک اخلاقی روی دستگاه‌های همراه به تدریس مشغول است، می‌گوید: «بسیاری از این برنامه‌ها به‌طور منظم دانلود شده‌اند، اما همچنان به رخنه‌ای آلوده هستند که با استفاده از یک گواهی جعلی TLS آن‌ها را آسیب‌پذیر می‌سازد.» بر طبق برآوردهای به عمل آمده، برنامه‌هایی که به آن‌ها اشاره شد تنها بخش کوچکی از برنامه‌های آندروید هستند که به احتمال زیاد این رخنه‌ها را در خود جای داده‌اند. همه پانزده برنامه‌ای که در تحقیق سام بان مورد بررسی قرار گرفتند، در سپتامبر گذشته از سوی مؤسسه نرم‌افزاری CERT Divisioبه‌عنوان برنامه‌های ناامن معرفی شدند. در یادداشت سپتامبر، محقق امنیتی، ویل دورمن به توسعه‌دهندگان CERT اعلام کرد توانسته است 23668 برنامه گرفتار این آسیب‌پذیری را شناسایی کند. بان برای شناسایی برنامه‌هایی که ویل دورمن درباره آن‌ها اطلاع‌رسانی کرده است، منبعی در اختیار ندارد. در نتیجه، به‌نظر می‌رسد بیش‌تر این برنامه‌ها همچنان بدون تغییر هستند. بان تحقیق روی این پروژه را زمانی آغاز کرد که در جریان کلاس متوجه شد تمام پیام‌های متنی منتقل شده توسط Snap Secure به‌راحتی می‌توانند توسط هر فردی با ارائه یک برنامه رمزگشایی شود که حاوی گواهی جعلی TLS است. برای آزمایش برنامه‌ها، دانشجویان بان از بسته نرم‌افزاری رایگان Burp و یک گواهی جعلی TLS برای اجرای یک حمله man-in-the-middle استفاده کردند. برنامه‌های آسیب‌پذیر آن‌هایی بودند که به این گواهی اطمینان و از کلید خصوصی موجود در آن برای رمزنگاری و رمزگشایی ارتباط استفاده کردند.
هکرها به نقاط مهم وای‌فای متصل می‌شوند، کارمندان درون ISP یا شبکه‌های خصوصی مجازی یا هکرهای تحت حمایت دولت که از ستون فقرات اینترنت استفاده می‌کنند، نیز می‌توانند از فناوری‌های مشابه برای مانیتور کردن یا اصلاح ارتباطات رمزنگاری شده بین دو برنامه آسیب‌پذیر و سروری استفاده کنند که این برنامه‌ها به آن متصل می‌شوند.

نداشتن اطمینان از ارتباطات HTTPS محافظت شده با استفاده از گوشی‌های هوشمند موضوع جدیدی نیست. نزدیک به 31 ماه پیش محققان آکادمیک برنامه‌هایی را شناسایی کردند که توسط صدها میلیون کاربر آندرویید دانلود شده بود. همه این برنامه‌ها از رخنه HTTPS مشابهی رنج می‌بردند. تحقیقات اخیر محققان از شکست نگران‌کننده رمزنگاری داده‌ها در ده‌ها هزار برنامه آی‌اواس خبر می‌دهد که در فروشگاه اپل قرار دارند. رخنه‌ها در هر دو گروه برنامه‌های آی‌اواس و آندرویید به‌شدت خطرناک هستند، به دلیل این‌که شناسایی این رخنه‌ها تقریباً برای کاربران نهایی این محصولات غیرممکن است. بر همین اساس، مقامات گوگل بیانیه‌ای را منتشر کرده‌اند: «برنامه‌هایی که آسیب‌پذیری در آن‌ها شناسایی شده در Google Play جایی ندارند. Google Play به طراحان درباره مسائل و مشکلات امنیتی بالقوه هشدار می‌دهد، ما اقدام‌های لازم را درباره یک‌سری از برنامه‌های خاص که در گذشته فعال بوده‌اند، انجام خواهیم داد. در خلال سال 2014، Google Play هشدارهایی را برای یک‌سری از سازندگان برنامه‌های بزرگ ارسال کرده است. (گزارش سالانه اخیر ما نشان می‌دهد بیش از 25 هزار برنامه بر اساس هشداری اصلاح شده‌اند که برای آن‌ها ارسال شد.) ما به‌زودی تصمیم‌های سخت‌گیرانه‌تری برای اصلاح گسترده این مسائل اتخاذ خواهیم کرد.» گوگل سعی می‌کند امنیت برنامه‌های ثالثی را که روی سرورهایش میزبانی می‌شوند، به شیوه مطلوبی بهبود بخشد. این شرکت نزدیک به 31 ماه به‌طور مداوم به‌صورت بی‌سر و صدا یا در بعضی موارد همراه با بیانیه‌ای برنامه‌های دارای نقص امنیتی را شناسایی کرده است.
همان طور که محققان آزاد اقدام به شناسایی رخنه‌ها در برنامه‌ها می‌کنند، محققان امنیتی گوگل و اپل نیز به شیوه مشابهی این کار را انجام می‌دهند. تا وقتی که محققان به فعالیت‌های خود می‌پردازند، کاربران بهتر است با احتیاط از برنامه‌ها استفاده کنند.

تاریخ انتشار:

25 خرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/853