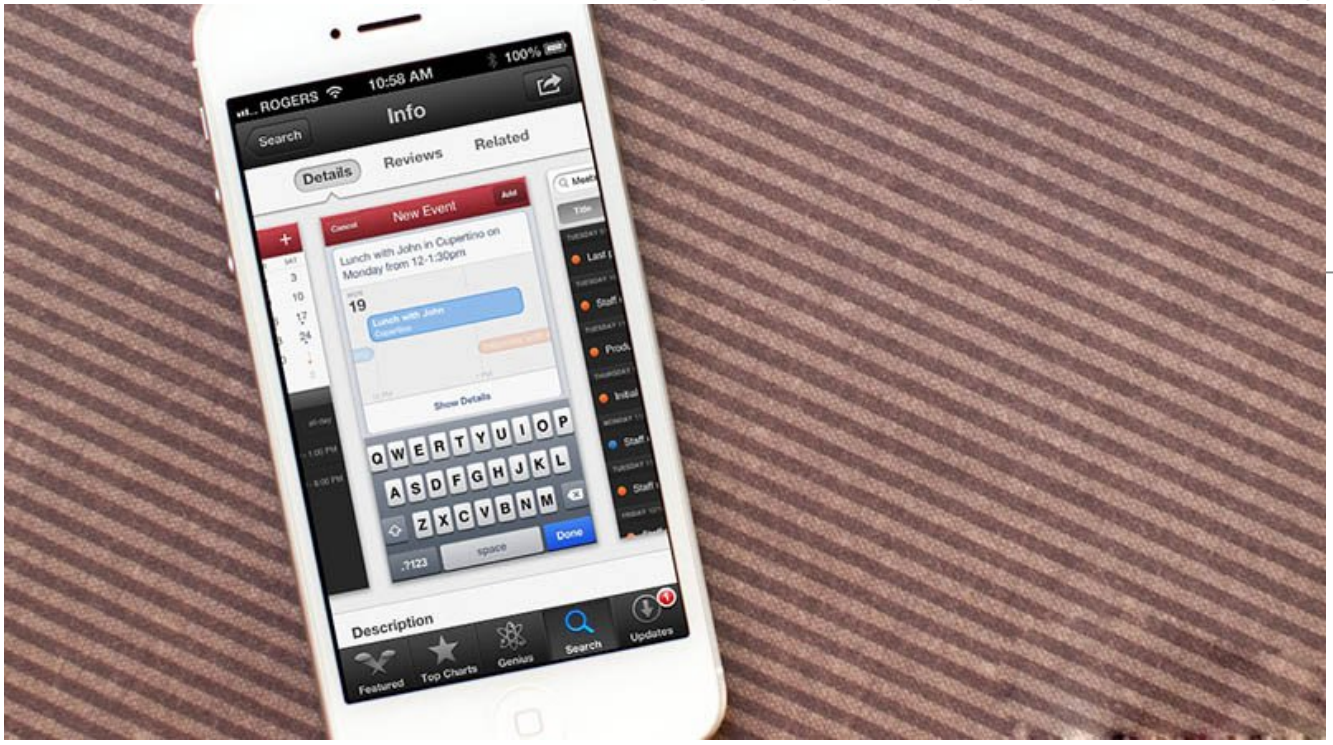
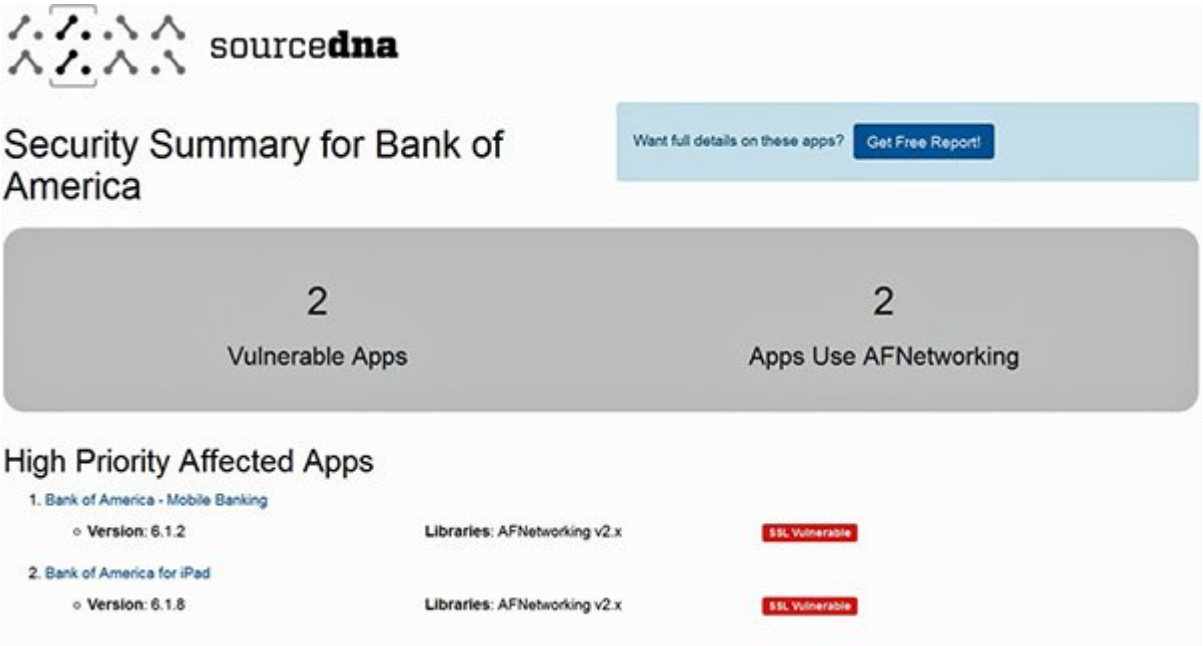
رخنه‌ای دیگر در HTTPS

متزلزل شدن امنیت هزاران کاربر آی‌اواس



هکرها توانایی اجرای یک حمله بالقوه را روی ترافیک رمزنگاری شده نزدیک به 25 هزار برنامه آی‌اواس دارند. این حمله به دلیل وجود آسیب‌پذیری در یک کتابخانه منبع باز شبکه که برنامه‌های آی‌اواس از آن استفاده می‌کنند، رخ می‌دهد. حمله مذکور به دلیل نداشتن اعتبارسنجی گواهی دیجیتال نام‌های دامنه در کتابخانه AFNetworking به‌وجود آمده است. AFNetworking کتابخانه‌ای است که برای برقراری ارتباط مورد استفاده طیف گسترده‌ای از برنامه‌های مک و آی‌اواس قرار دارد که شامل پروتکل HTTPS (پروتکل رمزنگاری شده HTTP) نیز می‌شود.

رخنه شناسایی شده به هکرها اجازه می‌دهد در یک مکان اقدام به رهگیری ترافیک HTTPS بین یک برنامه آسیب‌پذیر و یک سرویس وب، به‌منظور رمزگشایی آن با ارائه یک گواهی دیجیتال برای یک نام دامنه مختلف بپردازند. در نتیجه، یک حمله از نوع man-in-the-middle روی شبکه‌های بی‌سیم غیرایمن با هک کردن روترها یا با استفاده از روش‌های دیگر رخ دهد. آن گونه که شرکت SourceDNA، شرکتی که برنامه‌های جانبی عرضه شده برای تلفن‌های همراه را مورد ارزیابی قرار می‌دهد، گزارش می‌دهد: «این آسیب‌پذیری روی بیش از 25 هزار برنامه آی‌اواس قرار دارد، به دلیل این‌که این برنامه‌ها از نسخه 2/5/2 یا پایین‌تر کتابخانه AFNetworking استفاده می‌کنند.»
نیت لاوسون، مدیرعامل مؤسسه تحقیقات امنیت SourceDNA، در این باره می‌گوید: «این رخنه به دلیل این به وجود آمده که نام دامنه در cert مورد بررسی قرار نگرفته است. حتی اگر این موضوع باز هم توسط cert مورد بررسی قرار می‌گرفت، باید از وجود گواهی دیجیتال معتبر اطمینان حاصل پیدا می‌کرد. به‌طور مثال، من با دامنه sourcedna.com و با ارائه یک گواهی معتبر cert می‌توانم وانمود کنم Microsoft.com هستم.»
این رخنه در نسخه AFNetworking 3/5/2 که در تاریخ 20 آوریل عرضه شد، اصلاح شده است. SourceDNA در همین رابطه اعلام کرد: «برنامه‌هایی که گواهی سنجاق شده (Certificate pinning که در اصطلاح رایج آن را SSL pinning نیز می‌نامند) روی آن‌ها وجود داشته باشد، از این آسیب‌پذیری در امان هستند، اما این مکانیسم فقط توسط تعداد محدودی از طراحان در محصولاتشان مورد استفاده قرار گرفته است.» بر اساس بررسی‌های به عمل آمده توسط SourceDNA، برنامه‌های مورد استفاده توسط Wells Fargo، American Bank و JPMorgan Chase به احتمال زیاد آلوده شده‌اند. هرچند تعدادی از آن‌ها این گزارش را نادرست دانسته‌اند (شکل 1).



نکته جالب توجه درباره این رخنه به تاریخ 27 مارس بازمی‌گردد. درست یک روز بعد از آن‌که رخنه HTTPS-Scrippling که اجازه دسترسی تصدیق هویت نشده روی پروتکل HTTPS را در AFNetworking 2.5.2 امکان‌پذیر می‌ساخت، رخنه جدید شناسایی شد. این رخنه فقط روی نسخه 1/5/2 کتابخانه AFNetworking قرار داشت که نزدیک به 1500 برنامه از 100 هزار برنامه آی‌اواس را که از نسخه 1/5/2 کتابخانه AFNetworking استفاده می‌کردند، تحت تأثیر قرار داد. رخنه HTTPS-crippling به هکرها اجازه می‌داد تا به رهگیری گذرواژه‌های رمزنگاری شده، شماره حساب‌های بانکی و دیگر اطلاعات حساس بپردازند.
به دلیل افزایش این رخنه‌ها روی کتابخانه یاد شده، SourceDNA سرویس آنلاین Searchlight را راه‌اندازی کرد. کاربران می‌توانند از این سرویس برای بررسی و شناسایی آسیب‌پذیری نرم‌افزارهای آی‌اواس و آندرویید نصب شده روی دستگاه‌های همراهشان استفاده کنند. برای بررسی نرم‌افزار خود از نشانی http://sourcedna.com استفاده کنید. وقتی به صفحه این سایت وارد شدید، روی دکمه Check your Apps کلیک کنید. بررسی‌های به عمل آمده نشان می‌دهد برنامه‌هایی که توسط طراحان بزرگ همچون مایکروسافت، یاهو و گوگل طراحی شده‌اند، پتانسیل آلوده شدن به رخنه‌های AFNetworking را دارند.

تاریخ انتشار:
25 خرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/850