سایت‌های بزرگ در معرض تهدیدی جدید

باز هم شناسایی یک رخنه امنیتی خطرناک

شرکت‌ها و موسسات بزرگ داخلی و خارجی در معرض این تهدید امنیتی هستند. روز سه‌شنبه 3 مارس محققان امنیتی از وجود یک آسیب‌پذیری جدید در SSL/TLS که حمله FREAK نامیده می‌شود، خبر دادند.

FREAK به یک هکر اجازه رهگیری ارتباطات HTTPS میان سرورها و کلاینت‌های آسیب‌پذیر که از رمزنگاری ضعیفی استفاده کرده‌اند را می‌دهد که در ادامه به سرقت یا دستکاری داده‌ها منجر خواهد شد. FREAK اولین بار توسط کاتریکین بارگیون، محقق آزمایشگاه علوم کامپیوتر INRIA واقع در کشور فرانسه و miTLS شناسایی شد. اما متیو گرین اولین شخصی بود که در مقاله واشنگتن‌پست به افشاگری در مورد آن پرداخت. شرکت‌های فن‌آوری اطلاعات در تلاش برای رفع نقص امنیتی هستند که میلیون‌ها کاربری که از سایت‌های ایمنی همچون Whitehouse.gov ، NSA.gov و FBI.gov بازدید کرده‌اند را در معرض تهدید قرار داده است.

محققان امنیتی به یک نقص امنیتی که قدمت آن به دهه 90 میلادی باز می‌گردد و روی طیف گسترده‌ای از سیستم‌عامل‌های مورد استفاده کاربران همچون OS X، iOS، آندروید و ویندوز وجود دارد اشاره کردند. کاربران زمانی که به بازدید از سایت‌های بزرگ همچون آمریکن‌اکسپرس، Airtel، بلومبرگ، Groupon، Business Insider، Marriott و بسیاری دیگر می‌پردازند در معرض هک شدن قرار می‌گیرند. اکسپلویت FREAK به یک هکر اجازه می‌دهد با توانایی ویژه‌ای به یک سایت که از درجه رمزنگاری ضعیفی روی ارتباطات HTTPS استفاده می‌کند، وارد شود. این کار در کمتر از چند ساعت با استفاده از یک مجموعه کوچک از بات‌نت‌ها (تنها 75 کامپیوتر) انجام شود. زمانی که کرک انجام شد، هکرها توانایی هک کردن وب‌سایت‌ها و سرقت اطلاعات شخصی کاربران از سایت‌هایی که مورد بازید آن‌ها قرار گرفته است را دارند. به گزارش واشنگتن پست این مشکل به ضعف سیاست‌های ایالات متحده که در سال 1990 در زمینه رمزنگاری برای شرکت‌ها دیکته کرده بود باز می‌گردد.

نادیا هنینگر متخصص رمزنگاری در دانشگاه پنسیلوانیای می‌گوید: « برای سایت‌های آسیب‌پذیر روشی پیدا کرده است که در کمتر از هفت ساعت توانایی کرک کردن کلید رمزنگاری خارجی را با استفاده از کامپیوترهای سرویس‌دهنده خدمات وب آمازون دارد.»

جی آلکس هالدرمن و ذاکیر دورمریک محققان علوم کامپیوتر دانشگاه میگشیان می‌گویند: «بیش از یک سوم سایت‌های رمزنگاری شده که از سمبل قفل برای نشان‌دادن به کارگیری فن‌آوری SSL استفاده می‌کنند مورد بررسی قرار گرفته‌اند که ثابت می‌کند همه آن‌ها در معرض این آسیب‌پذیری قرار دارند. هالدرمن می‌گوید از 14 میلیون سایتی که در سرتاسر جهان از رمزنگاری استفاده می‌کنند، بیش از 5 میلیون از آن‌ها تا صبح سه‌شنبه همچنان آسیب‌پذیر باقی مانده‌اند.» متیو گرین و دیگر محققان می‌گویند: « به همه دولت‌ها، آژانس‌ها و شرکت‌های آلوده در هفته‌های گذشته اطلاع‌رسانی شده است به امید آن‌که، آن‌ها بتوانند قبل از آن‌که مشکل به صورت عمومی بروز پیدا کنند آن‌را برطرف نمایند.»

محققان امنیتی می‌گویند نقص ناشی از سیاست‌گذاری دولت امریکا در دهه 90 که شرکت‌ها را ملزم کرد به جای استفاده از رمزنگاری‌های قدرتمند از رمزنگاری‌هایی با درجه ضعیف و همچنین به کارگیری این رمزنگاری ضعیف در محصولاتی که به مشتریان کشورهای دیگر فروخته می‌شد، این مشکل را به وجود آورده است. البته این محدودیت‌ها در اواخر دهه 90 میلادی برداشته شد، اما رمزنگاری ضعیف به طور گسترده‌ای در نرم‌افزارهایی که در سرتاسر جهان و در خود ایالت متحده مورد استفاده قرار می‌گرفت به کار گرفته شد. به طوری که ظاهرا تا امسال نیز هنوز این رمزنگاری ضعیف مورد استفاده قرار می‌گرفته است. در آن موقع ایالات متحده حداکثر سطح رمزنگاری مورد استفاده را به رمزنگاری 512 بیتی محدود کرده بود. این سیاست که Crypto Wars نامیده شده است به ویژه در زمان مبارزات سیاسی برای استقرار یک الگوریتم رمزنگاری محدود مورد استفاده قرار می‌گرفت که به دولت امکان ردیابی مظنونین و شکستن رمزنگاری مورد استفاده توسط آن‌ها را می‌داد.

FREAK بیان‌گر یک روش حمله است که مخفف عبارت Factoring RSA-EXPORT Keys (حمله فاکتوری به کلید RSA) است. هر مرورگری که یک نسخه بدون وصله OpenSSL استفاده کند در معرض این تهدید قرار دارد که شامل مرورگرهای سافاری و هر دو سیستم‌عامل مک و iOS می‌شود. از اتفاق، سایت‌های پلیس فدرال آمریکا FBI، کاخ سفید و سازمان امنیت ملی امریکا NSA نیز در معرض این آسیب‌پذیری قرار دارند. بنابر گزارش‌ها دو سایت اولی وصله‌های لازم را در این خصوص دریافت کرده‌اند. فهرست سایت‌های معتبری که در معرض این آسیب‌پذیری قرار دارند در حال گسترش است. برای اطمینان از این که آیا سایتی که موردبازدید قرار داده‌اید جزء این موارد مشکوک به خطر بوده است یا نه، لینکی به فهرست کامل این سایت‌ها و همچنین نام چند سایت فارسی که اسم آن‌ها در این لیست به چشم می‌خورد در انتهای مقاله وجود دارد.

اپل نیز از وجود این آسیب‌پذیری در محصولات خود خبر داده است و گفته است هفته آینده یک وصله امنیتی را منتشر خواهد کرد. رایان جیمز سخنگوی این شرکت گفته است به‌روزرسانی نرم‌افزاری برای اصلاح این آسیب‌پذیری آماده شده است و در هفته آینده منتشر خواهد شد.

گوگل نیز بیانیه مشابهی را منتشر کرده است. لیز مارک من سخنگوی گوگل دراین باره می‌گوید: «گوگل برای رفع مشکل امنیتی FREAK که به هکرها امکان جاسوسی روی ارتباطاتی که توسط مرورگر آندروید گوگل برقرار می‌شود، وصله‌های لازم را برای دستگاه‌های گوشی‌هوشمند آماده کرده است.»

هنوز به درستی مشخص نیست آیا هیچ هکری اقدام به استفاده از این اکسپلویت کرده است یا نه اما بهتر است آخرین سایت‌هایی که از آن‌ها برای تراکنش‌های مالی خود استفاده کرده یا فعالیت‌های حساسی روی آن‌ها انجام داده‌اید را مورد بررسی قرار دهید.

مایکروسافت نیز به‌تازگی خبر از آسیب‌پذیری FREAK SSL در سیستم‌عامل ویندوز داد. باگ امنیتی FREAK به حمله‌کنندگان اجازه می‌دهد تا یک حمله Man in the middle را روی پروتکل‌های رمزنگاری SSL و TLS با استفاده از یک رمزنگاری غیرمرسوم انجام داده و یک فاجعه جدید را رقم بزنند. در این زمان SChannel (سرنام Microsoft Secure Channel) در معرض این تهدید قرار دارد. SChannel یک مجموعه نرم‌افزاری در ویندوز است که برای تأمین امنیت اطلاعات روی شبکه مورد استفاده قرار می‌گیرد. مایکروسافت به طور رسمی در سایت مشاوره امنیتی خود از وجود یک آسیب‌پذیری که برای دور زدن ویژگی امنیتی در SChannel مورد استفاده قرار گفته و روی خانواده سیستم‌عامل‌های ویندوز وجود دارد، خبر داده است. این آسیب‌پذیری از تکنیک Freak برای اکسپلویت کردن و افشای عمومی اطلاعات استفاده می‌کند که می‌تواند به یک مشکل جدی در حوزه صنعت و به ویژه سازمان‌های مالی ختم شود. دامنه این مشکل نیز محدود به یک سیستم‌عامل خاص نیست.

هرچند بخش تحقیقات مایکروسافت بخشی از تیم محققان اروپایی بود که برای اولین بار FREAK را کشف کردند بود، اما ردموند تصمیم گرفت خبر مربوط به این آسیب‌پذیری امنیتی را تا به امروز مخفی نگه دارد. در خبری که مایکروسافت در سایت خود قرار داده، اعلام کرده است تاکنون هیچ گزارشی مبنی بر مورد حمله قرار گرفتن کاربران بر اساس این آسیب‌پذیری دریافت نکرده است.

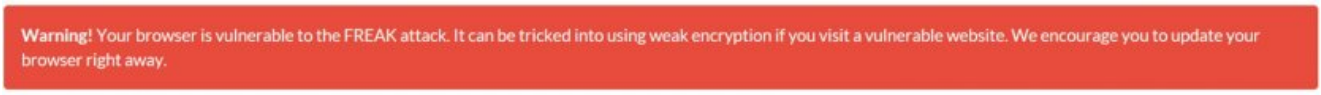
مایکروسافت می‌گوید: « به طور مستمر در حال کار هستیم و از طریق برنامه MAPP (سرنام Microsoft Active Protection Program) که برنامه‌ای برای اطلاع‌رسانی درباره آسیب‌پذیری‌ها و به‌روزرسانی‌های مربوطه است از شرکای خود محافظت می‌کند و هر زمان وصله‌ای آماده شد یا اطلاعیه امنیتی مهمی وجود داشته باشد، با اطلاع‌رسانی از مشتریان خود محافظت می‌کند.» مایکروسافت همچنین درباره زمان عرضه وصله امنیتی مربوطه گفته

است بسته به نیاز مشتریان این وصله امنیتی می‌تواند در قالب برنامه ارائه ماهیانه وصله‌های امنیتی یا خارج از چرخه به‌روزرسانی‌ها منتشر شود.

سیستم‌عامل‌هایی که به این آسیب‌پذیری آلوده شده‌اند عبارتند از ویندوز سرور 2003، ویندوز ویستا، ویندوز سرور 2008، ویندوز 7، خانواده ویندوز 8، ویندوز سرور 2012 و ویندوز RT. مایکروسافت می‌گوید: «کاربران می‌توانند تبادل رمز کلید RSA را که باعث بروز FREAK می‌شود با تغییر SSL Chiper Suite در Group Policy Object Editor غیرفعال کنند، مگر آن که از سیستم‌عامل ویندوز سرور 2003 که اجازه فعال یا غیرفعال کردن رمزنگاری‌های شخصی را نمی‌دهد، استفاده کنند. خانواده ویندوزهای سرور به شرطی که روی پیکربندی پیش‌فرض قرار داشته باشند به دلیل این که امکان ارسال رمزنگاری در آن‌ها غیرفعال است در معرض این حمله قرار ندارند.»

در زمان نگارش این مقاله فهرستی از مرورگرهای وب همچون اینترنت‌اکسپلورر، کروم، آندروید، مرورگر آندروید، سافاری، iOS، Mac OS X، مرورگر بلک‌بری، اپرا ویژه سیستم‌عامل آندروید و مک در فهرست سایت freakattack.com قرار دارند.

کاربران برای اطمینان از این موضوع که آیا مرورگر آن‌ها آلوده است یا خیر می‌توانند از ابزار FREAK Client Test Tool استفاده کنند. زمانی که به این سایت مراجعه کنید اگر مرورگر شما به این آسیب‌پذیری آلوده باشد پیغام زیر را مشاهده خواهید کرد. پیغام زیر آلودگی در نسخه 10 مرورگر اینترنت‌اکسپلورر را نشان می‌دهد.



Cipher Suite

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_RC4_128_MD5

اگر مرورگر شما به این آسیب‌پذیری آلوده نباشد پیغام زیر را مشاهده خواهید کردد. (مرورگر کروم نسخه 32)

(Cipher به روشی برای تبدیل plain text به متنی که معنای آن پنهان باشد گفته می‌شود.)

مرورگر فایرفاکس نسخه 37 نیز از این آلودگی در امان است.

Cipher Suite

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_RC4_128_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_RC4_128_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

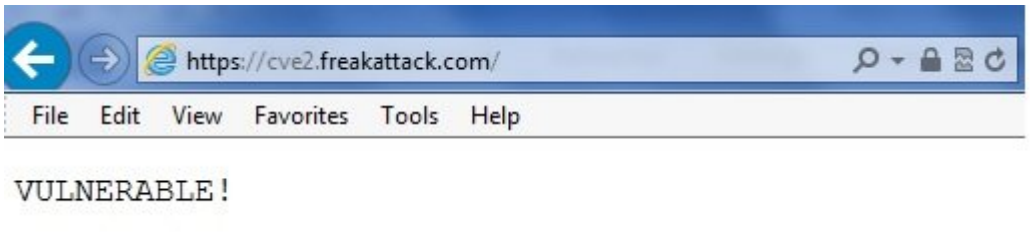
TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

برای طراحان نیز ابزارهایی برای تست برنامه‌هایشان وجود دارد. برای این منظور می‌توانید از ابزارهایی که وضعیت ماشین را در سطح پایین مورد بررسی قرار می‌دهند، استفاده کنید. برای منظور از دو آدرس زیر می‌توان استفاده کرد. با مراجعه به هر یک از این آدرس‌ها اگر ارتباط بدون مشکل برقرار باشد به معنای آسیب‌پذیری است.



در غیر این صورت پیغامی مبنی بر عدم دسترسی به ارتباط SSL مشاهده می‌کنید.

فهرست کامل سایت‌ها

منابع: 1 + 2 + 3 + 4 + 5

تاریخ انتشار:

17 اسفند 1393

نشانی منبع: https://www.shabakeh-mag.com/news/world/377