بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی یک آسیب‌پذیری در کلید رمزنگاری تراشه‌های Wi-Fi

اسفند ۹۸

فهرست مطالب

۱ چکیده

به گفته محققان آزمایشگاه‌های تحقیقاتی ESET، اخیراً یک آسیب‌پذیری جدی در تراشه‌های Wi-Fi کشف شده است که میلیاردها دستگاه در سراسر جهان را تحت تأثیر قرار می‌دهد. آسیب‌پذیری KrØØk مربوط به یک کلید رمزگذاری تمام صفر در تراشه‌های Wi-Fi است که ارتباطات دستگاه‌های آمازون، اپل، گوگل، سامسونگ و دیگر دستگاه‌ها را افشا می‌کند. این آسیب‌پذیری، به مهاجمان امکان می‌دهد تا بتوانند ارتباطات Wi-Fi را شنود کنند. در ادامه به بررسی بیشتر این آسیب‌پذیری خواهیم پرداخت.

۲ محصولات تحت تاثیر

تراشه‌های Wi-Fi آسیب‌پذیر در تلفن‌های هوشمند، تبلت‌ها، لپ‌تاپ‌ها (که از سیلیکون Broadcom استفاده می‌کنند) و در دستگاه‌های اینترنت اشیا (تراشه های Cypress)، از جمله چندین نسل از محصولات آمازون (اکو ، کیندل)[۱]، اپل (آی‌فون، آی‌پد، مک‌بوک)، گوگل (نکسوس)، سامسونگ (گلکسی[۲])، رزبری (پی۳)، شیائومی (ردمی[۳]) یافت می‌شوند. همچنین محققان، این اشکال را در نقاط دسترسی (AP) و مسیریاب‌های ایسوس و هوآوی مشاهده کرده‌اند. در کل تخمین زده می‌شود که بیش از یک میلیارد دستگاه از این آسیب-پذیری متاثر می‌شوند.

۳ تاثیر آسیب پذیری

به گفته محققان ESET، این آسیب پذیری که با شناسه CVE-2019-15126 شناخته می‌شود، در نتیجه استفاده از کلید رمزنگاری تمام صفر در تراشه‌های ساخته شده توسط Broadcom و Cypress ناشی می‌شود. آسیب‌پذیری مذکور، موجب رمزگشایی داده‌ها شده و پروتکل‌های امنیتی WPA2-Personal و WPA2-Enterprise را می‌شکند.

[۱] Echo, Kindle
[۲] Galaxy
[۳] Redmi

۴ مشخصه‌های آسیب‌پذیری

محققان نام این آسیب پذیری را "KrØØk" گذاشته‌اند تا هم از ترکیب صفرها استفاده کرده باشند و هم به این دلیل که آن را مربوط به حمله KRACK می‌دانند. حمله KRACK یک حمله نصب مجدد کلید بود که در سال ۲۰۱۷ کشف شد. رویکرد KRACK به این صورت بود که یک مشکل گسترده صنعتی در پروتکل‌های WPA و WPA2 برای تأمین امنیت Wi-Fi بود که می‌توانست منجر به از دست رفتن کامل کنترل روی داده‌ها شود. این حمله، به یک مهاجم این امکان را می‌داد که بتواند حمله MITM را به اجرا در آورده و در آن محدوده رادیویی، امکان بازپخش، رمزگشایی یا جعل ساختارها[۴]را داشته باشد. به گفته محققان، KrØØk می‌تواند یکی از گزینه‌های ممکن برای نصب مجدد یک کلید تمام صفر باشد که در حملات KRACK مشاهده شده بود.

۴-۱ جزئیات آسیب‌پذیری

در ارتباطات Wi-Fi، هر زمان که دستگاهی به یک نقطه دسترسی (AP) وصل شود، به آن تجمیع گفته می‌شود. به حالت قطع اتصال (به عنوان مثال هنگامی که شخص از یک Wi-Fi AP به دیگری منتقل می‌شود، تداخل سیگنال را تجربه می کند یا Wi-Fi در دستگاه خاموش می‌شود)، عدم تجمیع گفته می‌شود.

به گفته محققان، آسیب‌پذیری KrØØk پس از یک عدم‌تجمیع اتفاق می‌افتد. در این حالت، کلید جلسه ذخیره شده در تراشه Wi-Fi کنترل‌کننده رابط شبکه بی‌سیم (WNIC[۵]) در حافظه پاک شده و روی صفر تنظیم می‌شود. این رفتار مورد انتظار است؛ زیرا پس از عدم تجمیع، قرار نیست هیچ اطلاعات دیگری انتقال یابد. با این حال، تمام ساختارهای داده‌ای که در بافر انتقال تراشه باقی مانده‌اند، پس از رمزگذاری با این کلید تمام صفر منتقل می شوند. از آنجا که از کلید تمام صفر استفاده می‌شود، این رمزگذاری، در واقع منجر به رمزگشایی داده‌ها و تبدیل آن‌ها به متن آشکار می‌شود.

روش حمله ساده است: حالات تجمیع و عدم‌تجمیع، توسط ساختارهای مدیریتی اداره می‌شوند ، که خود احراز هویت نشده و بدون رمز هستند. برای سوءاستفاده از این آسیب‌پذیری، یک مهاجم می‌تواند با ارسال یک ساختار داده مدیریتی دستکاری شده، به طور دستی یک عدم‌تجمیع ایجاد کند و سپس قادر به بازیابی اطلاعات باقیمانده در بافر به صورت متن آشکار، باشد.

---

[۴] Frames

[۵] Wireless Network Interface Controller

آسیب‌پذیری KrØØk می‌تواند ۳۲ کیلوبایت داده را به یک‌باره افشا کند، که معادل حدود ۲۰،۰۰۰ کلمه است. یک مهاجم می تواند مجموعه‌ای از ساختارهای مدیریتی را برای بهره‌برداری از این آسیب‌پذیری، به صورت مداوم ارسال کرده و شروع به جمع‌آوری داده‌ها کند. در نتیجه این کار، مهاجم می‌تواند رمزهای عبور، اطلاعات کارت اعتباری یا هر چیز دیگری که کاربر ممکن است از طریق Wi-Fi در حال ارسال باشد، دریافت نماید.

عمل شنود، می‌تواند به صورت فعال یا غیرفعال باشد. آنچه مهاجمان از ارتباطات می‌شنوند، بستگی به زمان دارد که در آن زمان کاربر چه کاری انجام می‌دهد. مهاجم می‌تواند در میان کارهای همیشگی کاربر، منتظر اطلاعات جالبی باشد تا بتواند از آن سوءاستفاده کند.

این حمله زمانی بزرگتر می‌شود که یک نقطه دسترسی آسیب‌پذیر در این ترکیب دخیل باشد. به عنوان مثال، گوش دادن به یک هاب خانگی هوشمند[۶] می تواند اطلاعاتی را که بین آن و دستگاه‌های ماهواره‌ای از قبیل یک ترموستات هوشمند، چراغ‌های هوشمند، لپ‌تاپ، رایانه و دستگاه‌های تلفن همراه، ارسال می‌شود، بازیابی کند. محققان توضیح داده‌اند که این امر به مهاجمان اجازه می‌دهد حتی دستگاه‌های غیرآسیب‌پذیری یا وصله شده را شنود کنند. این امکان، دامنه جمله را به شدت گسترش می‌دهد، طوری که یک مهاجم فقط می‌بایست یک ساختار مدیریتی به نقطه دسترسی ارسال کرده و سپس می‌تواند به کل محیط دسترسی پیدا کند.

محققان در یک نسخه نمایشی، نشان دادند که آسیب‌پذیری KrØØk می‌تواند برای بازیابی رمزهای عبور دستگاه‌های غیرآسیب‌پذیر متصل به یک نقطه دسترسی آسیب‌پذیر استفاده شود. به این ترتیب، این اشکال به مهاجمان اجازه می دهد تا بتوانند اختیار کل خانه یا کل دفتر را به دست آورند.

۵ اقدامات جهت کاهش شدت آسیب پذیری

محققان مسئولانه این آسیب‌پذیری را افشا کرده و یک دوره ۱۲۰ روزه به Broadcom و Cypress برای ایجاد بروزرسانی‌های firmware فرصت داده‌اند. در ضمن به تولیدکنندگان فرصت داده شده است تا در بروزرسانی سیستم‌عامل‌ها، ایجاد وصله‌ها و بهبود firmwareها اقدامات لازم را انجام دهند و این بروزرسانی‌ها را در اختیار کاربران قرار دهند.

[۶] Smart home hub

اصلاحات لازم توسط تولیدکنندگان اصلی منتشر شده است و کاربران برای اطمینان از اینکه ارتباطات از دستگاه‌های Wi-Fi شان به راحتی قابل هک نباشند، لازم است دستگاه‌های خود را پس از انتشار بروزرسانی توسط تولیدکنندگان بروز نمایند.

۶ منابع

[1] https://threatpost.com/billions-of-devices-wifi-encryption-hack/153267/

[2]https://threatpost.com/krack-vulnerability-puts-medical-devices-at-risk/131552/