موضوع :

آشنایی با حمله KRACK و راه های مقابله با آن

(برای مشترکین)

مقدمه

محققان امنیتی چندین آسیب پذیری کلید مدیریتی را در هسته Wi-Fi Protected Access II که به اختصار WPA2 نامیده می شود را کشف کردند.

WPA2 یک روش احراز هویت ۱۳ ساله است که بصورت گسترده ایی جهت امن سازی ارتباطات بیسیم استفاده در می شود، اما این استاندارد در معرض خطر قرار دارد و این خطر تقریبا تمامی دستگاهای Wi-Fi از جمله مودم های مورد استفاده در خانه ها و محل های کار را در بر می گیرد.

مهاجمان می تواند از این آسیب پذیری با استفاده از حملات بازسازی کلید (KRACK) بهره برداری کنند و برای خواندن اطلاعاتی که پیش از این تصور می شد به طور ایمن رمزگذاری شده است، استفاده کنند.

اثبات این حمله توسط یک تیم از محققان که علیه امنیت مودم های بیسیم کار می کنند انجام شد و نشان داده شد که چگونه این حمله می تواند برای سرقت اطلاعات حساس نظیر شماره کارت های بانکی ،پسورد ها ، چت ها ،ایمیل ها و تصاویر مورد سوء استفاده قرار بگیرد.

این حمله علیه تمام شبکه های Wi-Fi محافظت شده مدرن امکان پذیر است و بسته به پیکربندی شبکه، امکان تزریق و دستکاری داده ها نیز وجود دارد. به عنوان مثال، مهاجم ممکن است قادر به تزریق ransomware یا دیگر نرم افزارهای مخرب به وب سایت ها باشد.

از آنجایی که این نقاط ضعف در هسته ی استاندارد wifi هستند و نه در نحوه ی پیاده سازی آن یا محصول یک شرکت خاص، بنابر این حتی پیاده سازی های صحیح WPA2 هم در خطر هستند.

مطابق گفته ی محققان ، این حمله بروی موارد زیر عمل می کند:

۱. هردو استاندارد WPA1 وWPA2
۲. شبکه های شخصی (Personal) و یا سازمانی(enterprise)
۳. الگوریتم های رمز گذاری WPA-TKIP و AES-CCMP وGCMP

به زبان ساده ، اگر مودم شما بی سیم است ، به احتمال بسیار زیاد آسیب پذیر است. در طول تحقیقات اولیه ،محققان کشف کردند که دستگاه های اندروید ،لینوکس،ویندوز ، OpenBSD، MediaTek، Linksysو ... تماما تحت تاثیر حمله KRACK هستند.

نکات قابل توجه در خصوص این آسیب پذیری

۱. این آسیب پذیری بخاطر نقص در پروتکل WPA2 بوده و فقط با به روز رسانی هایی که سازندگان تجهیزات انتهایی مانند کامپیوترها و لپ تاپ ها و گوشی های هوشمند و مودمها قابل کنترل می باشد.
۲. نیازی به ارتقاء به WPA3نیست و با Patch کردن دستگاه ها می توان تا حد زیادی از این حمله پیشگیری کرد.
۳. تغییر رمز عبور شبکه Wi-Fi شما باعث جلوگیری (یا کاهش) حمله نمی شود. بنابراین مجبور نیستید رمز عبور شبکه Wi-Fi خود را به روز کنید. در عوض، باید اطمینان حاصل شود تمام دستگاه ها به روزرسانی می شوند و همچنین باید سیستم عامل روتر خود را به روز کنید. با این وجود، پس از به روز رسانی هر دو دستگاه سرویس گیرنده و روتر خود، تغییر رمز عبور Wi-Fi اید بدی نیست.
۴. استفاده از WPA2 با رمزنگاری AES هم آسیب پذیر است. این حمله علیه WPA1 و WPA2، در برابر شبکه های شخصی و سازمانی، و در برابر هر مجموعه رمز که مورد استفاده قرار می گیرد (WPA-TKIP، AES-CCMP و GCMP) کار می کند. بنابراین هر کس باید دستگاه های خود را برای جلوگیری از حمله به روز رسانی کند!
۵. قرار است استاندارد Wi-Fi برای جلوگیری از این حملات بروز شود. این به روز رسانی ها احتمالا با پیاده سازی های قدیمی WPA2 سازگار خواهند بود.

اقدامات و توصیه های امنیتی در خصوص این آسیب پذیری

۱. کلیه دستگاه ها و تجهیزاتی که با WiFi کار می کنند شامل کامپیوترها و لپ تاپ ها و گوشی های هوشمند و مودمها را بطور مداوم بروز رسانی کنید تا Patch های منتشر شده برای رفع این آسیب پذیری بر روی دستگاه های شبکه نصب شود.
۲. به‌جای HTTP از HTTPS استفاده کنید.
۳. اطلاعات محرمانه را روی ارتباطات رمزگذاری نشده قرار ندهید.
۴. تا زمانی‌که مجبور نشده‌اید از شبکه‌های وای‌فای عمومی استفاده نکنید.
۵. از وبسایت‌های ناشناس بازدید نکنید و از منابع نامطمئن، نرم‌افزار نصب نکنید.

اقدامات و توصیه های امنیتی کلی برای امن کردن شبکه خانگی

۱. استفاده از رمزنگاری(Encryption) برای امنیت وایرلس مودم
رمزنگاری WEP قدیمی ترین و ضعیف ترین مدل رمزنگاری است. به جای آن از WPA و WPA-2 استفاده کنید. همچنین می‌توانید از الگوی AES یا TKIP نیز استفاده کنید. فقط در نظر داشته باشید که شکستن قفل ۲۵۶ بیتی به مراتب سخت‌تر و زمان‌برتر از شکستن رمز ۱۲۸ بیتی است.
۲. استفاده از یک رمز قوی برای اتصال وایرلس ، رمزی که بلند باشد و از ترکیب حروف کوچک و بزرگ و اعداد و نشانه‌های خاص تشکیل شده باشد.
۳. Firmware مودم را به روز کنید.
۴. رمز عبور ادمین را عوض کنید.

هر مودمی یک رمز عبور پیش فرض دارد که برای دسترسی به تنظیمات آن مورد استفاده قرار می گیرد. بیشتر ویزاردهای نصب و راه اندازی مودم شما را مجبور به عوض کردن آن می کنند اما نه همه آنها. در هر صورت رمز عبور را عوض کنید تا مانع از هک شدن سریع و آسان مودم خود شوید. رها کردن دستگاه به همین صورت، راه دسترسی غیر مجاز به تنظیمات مودم، به‌ویژه برای کسانی که دستگاه‌های مشابه دارند را افزایش می‌دهد.

۵. به تنظیمات پیش فرض برگردید

اگر رمز عبور مودم خود را فراموش کردید می توانید برای رهایی از این مشکل مودم خود را به حالت پیش فرض برگردانید. این کار با نگه داشتن دکمه Reset Factory به مدت ۳۰ ثانیه قابل انجام است ضمن اینکه بعد از ریست کردن به حالت پیش فرض و به منظور دسترسی به تنظیمات مودم نیاز به نام کاربری و رمز عبور پیش فرض مودم دارید که هر دو آن را می توانید دردفترچه راهنمای مودم بدست بیاورید.

۶. SSID Broadcast را غیر فعال کنید.

وقتی SSID Broadcast فعال است مودم اسم وایرلس- اسم شبکه - را پخش می کند که به همسایگان اجازه می دهد تا شبکه شما را ببینند و شاید هم اقدام به دسترسی به آن نمایند. برای جلوگیری از این موضوع broadcasting را غیر فعال کنید تا باعث شود SSID شما مخفی بماند. در این صورت برای دسترسی به وایرلس خود به قسمت unnamed networkرفته و SSID شبکه خود را وارد کنید.

توجه کنید: برخی از مودم ها امکان «مخفی‌کردن» خود را به کاربر می‌دهند. به‌طوری که دستگاه‌های بی‌سیم دیگر نام این شبکه ها را در فهرست شبکه های موجود در اطراف نشان نمی‌دهند. این روش برای دورماندن از حملات نفوذی چندان کارساز نیست. با «مخفی‌کردن» تنها آن را از نگاه کاربران معمولی و دستگاه‌های اطراف مخفی می‌کنید. نرم‌افزارهایی وجود دارند که با آنها به راحتی می‌توان هویت شبکه های «مخفی» را کشف کرد.

۷. همچنین در بعضی از مودمها می‌توان قدرت فرکانس ارسالی را تغییر داد. با کم کردن قدرت امواج، درست است که برای وصل‌شدن به اینترنت باید به دستگاه نزدیک‌تر باشید، اما دست‌کم نفوذ به شبکه بی‌سیم از فاصله زیاد را دشوارتر می‌کنید.

۸. SSID پیش فرض مودم را عوض کنید.

SSIDپیش فرض مودم (برای مثال Linksys) راعوض کنید . وقتی آن را به حال خود رها می کنید به مردم دنیا اعلام می کنید که مودم خود را از نظر امنیتی پیکر بندی نکرده اید و هکر ها را طلب می کنید.

۹. با MAC address فیلتر کنید

می توانید مودم خود را با استفاده از MAC طوری فیلتر کنید که فقط کامپیوترهای شما بتوانند به شبکه وصل شوند. اکثر مودم ها، کامپیوتر ها و اسمارت فون هایی را که به شبکه شما وصل هستند را نشان می دهند. با اضافه کردن MACآن ها دسترسی غیرمجاز دیگر سیستم ها را به مودم قطع می کنید.

روش یافتن مک‌آدرس در دستگاه‌های مختلف متفاوت است. کافی است در موتور جست‌وجو (گوگل، یاهو ...) عبارت How to find mac address in ... (windows, iphone ...)را جست‌وجو کنید.

۱۰. تعداد کلاینت های DHCP را کم کنید.

اکثر کاربران از مودم خود به عنوان سرور DHCP استفاده می کنند وقتی کاربران وصل می شوند مودم به صورت خودکار یک آدرس IPبه هر یک از آنها اختصاص می دهد. با کم کردن تعداد IP های موجود (به تعداد کلاینت های موجود در خانه) باعث می شوید نفر دیگری نتواند خود را به شبکه تحمیل کند.

۱۱. استفاده از فایروال مودم

بسیاری از مسیریاب‌ها فایروال دارند و تنها کافی است آن را فعال کنید. حداقل ویژگی فعال‌بودن فایروال این است که از شبکه شما تا حد زیادی در برای حمله‌هایی چون (DoS) محافظت می‌کند.

۱۲. اجازه‌ی کنترل از راه دور به مسیریاب (Router) را غیر فعال کنید

امکان کنترل از راه دور Remote Access یا Remote Management برخی از مسیریاب‌ها به صورت پیش‌فرض فعال است. بهتر است این امکان را خاموش کنید چرا که با این کار امکان دسترسی به تنظیم‌های مسیریاب خود از طریق اینترنت را از بین می‌برید.

۱۳. در صورت عدم استفاده طولانی از مودم انرا خاموش کنید.

۱۴. علاوه بر نکات یادشده اقدامات دیگری هم برای بالا بردن امنیت مسیریاب‌ها وجود دارد که بسته به نوع فعالیت کاربران و البته دانش فنی آنان نسب به آن‌چه انجام می‌دهند، قابل اجرا هستند. مثلا می‌توان استفاده از درگاه‌های (Port) خاص را مسدود یا محدود کرد و جلوی برخی از خدمات و فعالیت‌ها را گرفت.

در مجموع امنیت دیجیتال نه صرفا با داشتن نرم‌افزارهای ویژه محقق می‌شود و نه با بالا بردن ایمنی سخت‌افزاری. در دنیای مجازی «امنیت مطلق» اساسا وجود ندارد. این شیوه‌ها تنها مسیر نفوذ به اطلاعات را سخت‌تر می‌کنند. در نهایت این کاربر است که با رفتار خود از داده‌های حساس حفاظت می‌کند یا آنها را در دسترس دیگران قرار می‌دهد.

اقدامات امنیتی عمومی بر روی کامپیوترها و گوشی های هوشمند

۱. تهیه نسخه پشتیبان: از اطلاعات سیستم به صورت دوره ای نسخه پشتیبان تهیه کنید.

۲. محدود کردن سطح دسترسی کاربران

۳. بروزرسانی و نصب اصلاحیه ها (Patch) در اولین فرصت ممکن و استمرار در انجام آن هم برای سیستم عامل و هم برنامه های کاربردی. شایان ذکر است بسیاری از بهره جویی ها از طریق سوءاستفاده از ضعف های امنیتی نرم افزارهای پرکاربردی نظیر Adobe Flash، Office و مرورگرها صورت می پذیرد. هر چه زودتر اصلاحیه نصب شود آسیب کمتری متوجه شما می شود.

۴. استفاده از فناوری های حفاظتی پیشرفته: استفاده از ضدویروس قدرتمند و به روز جهت مقابله با بد افزارها ضروری است.

۵. غیرفعال کردن بخش ماکرو : با توجه به انتشار بخش قابل توجهی از بد افزارها از طریق فایلهای نرم افزار Office حاوی ماکروی مخرب، غیرفعال کردن بخش ماکرو برای کاربرانی که به این قابلیت نیاز ندارند با فعال کردن گزینه Disable all macros without notification توصیه می شود.

۶. احتیاط در زمان باز کردن ایمیلها: صرفنظر کردن از فایلهای حتی کمی مشکوک و باز نکردن آنها می تواند نقشی مؤثر در پیشگیری از اجرا شدن فایلهای مخرب داشته باشد.

۷. خاموش کردن یا قطع استفاده از اینترنت در زمان عدم استفاده از دستگاه

۸. آگاه بودن در خصوص روشهای جدید هک و آسیب پذیریهای دستگاه ها و برنامه ها: هکرها دائما در حال تغییر و تکامل روش های خود هستند. با مرور اخبار از آخرین روشهای مورد استفاده مهاجمان آگاه شده و سیاستهای پیشگرانه لازم را اعمال کنید.

جهت اطلاعات بیشتر و گزارش موارد با امور امنیت شبکه و فناوری اطلاعات تماس حاصل فرمایید.