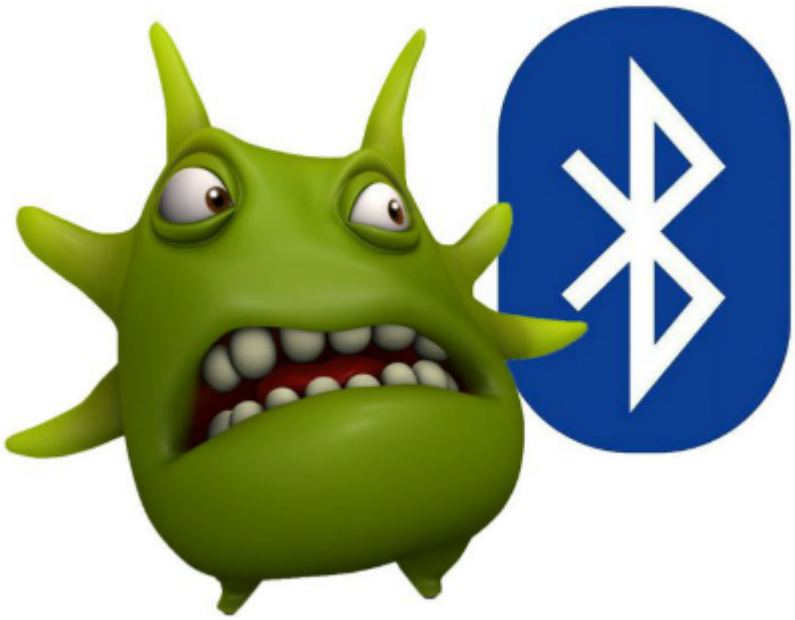
حفره امنیتی ارتباطات بلوتوث و امکان سرقت اطلاعات حساس توسط هکرها - دیجیاتو

محسن خوشنود | چهارشنبه، ۰۳ مرداد ۱۳۹۷

زمانی که دو دستگاه مجهز به بلوتوث را با یکدیگر جفت (Pair) می کنید، این دو ابزار (مثلاً موبایل و کامپیوتر) کلیدهای رمزنگاری شده ای را با یکدیگر به اشتراک می گذارند. اما بر اساس پژوهش های جدید، به نظر می رسد که نیاز نیست هر دو سوی ارتباط کلیدها را تأیید کنند که این موضوع، باعث به وجود آمدن یک حفره امنیتی می شود.

حفره مورد بحث اخیراً زمانی که یک هکر توانست در ارتباط میان دو دستگاه بلوتوث نفوذ کند پیدا شد و توجه متخصصان حوزه امنیت را به خود جلب کرد. البته اگر یکی از ابزارهای مورد استفاده پارامترهای رمزنگاری را بررسی و تأیید کند، خطر حمله به شدت کاهش خواهد یافت. همچنین هکر باید در فاصله مناسب (چند ده متری) برای برقراری ارتباط بلوتوث حاضر باشد.



با این حال شرکت های مختلف تا کنون با ارائه به روزرسانی های نرم افزاری تلاش کرده اند جلوی حفره امنیتی مورد بحث را تا جای ممکن بگیرند. کمپانی اپل ایراد مذکور را در نسخه «El Capitan» مک و پس از آن برطرف کرده و مایکروسافت نیز برای سیستم عامل های ویندوز 7، ویندوز 8.1 و ویندوز 10 بسته امنیتی متناسب را عرضه نموده است.

بسیاری از شرکت ها با ارائه بسته های امنیتی حفره امنیتی بلوتوث را در محصولات خود

مسدود کرده اند

البته بسته به نوع دیوایس، تولیدکننده سخت افزار نیز باید به روزرسانی هایی ارائه کند که شرکت برادکام ماه گذشته با یک پچ وظیفه خود را در این زمینه انجام داد. هرچند این گونه پچ های نرم افزاری نیازمند دستکاری برای عملکرد درست در دستگاه های مختلف هستند که شرکت هایی مانند دل و لنوو تغییرات لازم را در آپدیت های خود اعمال کرده اند.

لازم به ذکر است که ایراد امنیتی بلوتوث مربوط به بخش تبادل فایل بوده و به عنوان مثال در هنگام اتصال دسته ایکس باکس به کامپیوتر، کاربر را در معرض خطر قرار نمی دهد. اما از آنجایی که انتقال اطلاعات از طریق بلوتوث (به صورت مکمل برای سایر راه های ارتباطی مانند وای فای) روز به روز فراگیرتر می شود، متخصصان حوزه امنیت به کاربران توصیه می کنند همواره آخرین آپدیت ها را برای لوازم الکترونیکی خود دریافت نمایند.

دیجیاتو