هک قفل‌های هوشمند توسط بلوتوث

بررسی‌های کارشناسان امنیتی روی ۱۶ نمونه قفل هوشمند نشان می‌دهد که این تجهیزات در برابر حمله مهاجمان بسیار نا امن هستند.

به گزارش واحد امنیت سایبربان؛ در اجلاس دف کان(DEF CON) ، کارشناسان به بررسی قفل‌های هوشمند پرداختند که در این میان مشخص گردید ۷۵ درصد از تجهیزات مذکور، مستعد هک هستند. بررسی‌ها نشان می‌دهد که شرکت‌های تولیدکننده قفل‌های هوشمند مانندCeomate ، Vians، Quicklockدر برابر حملات هکری صورت گرفته توسط مهاجمان در معرض خطر قرار دارند. باوجود حملات صورت گرفته روی تجهیزات موردنظر، کارشناسان در تلاش برای تهیه زیرساخت‌های موجود برای امن کردن تجهیزات خانه‌های هوشمند هستند.

در این اجلاس مهندسان برق و کارشناسان خانه‌های هوشمند، به تحلیل و بررسی ۱۶ نمونه از این قفل ها پرداختند که مشخص شد، حداقل ۱۲ نمونه از قفل‌ها، با استفاده از دسترسی بی‌سیم قابل هک هستند.

کارشناسان در تحقیقات خود این‌چنین اعلام می‌کنند که برای رفع این آسیب‌ها در تجهیزات نام‌برده تاکنون اقدامی صورت نگرفته است و سازندگان این تجهیزات، تمایلی به برطرف کردن این آسیب در زیرساخت‌های خود ندارند. بنابراین شناسایی این آسیب‌پذیری‌ها در تجهیزات هوشمند ساختمان‌ها، برای کاربران بسیار نگران‌کننده است. علاوه بر این، کارشناسان پس از بررسی‌های خود به این نتیجه رسیدند که مدل قفل‌های Doorlock و Quicklock از بیشترین آسیب‌پذیری‌ها برخوردار هستند. بررسی‌ها نشان می‌دهد که پس از واردکردن رمز عبور توسط مهاجم به صورت مکرر، دسترسی کاربر اصلی از قفل نیز گرفته می‌شود. فروشندگان و کارشناسان امنیتی به کاربران توصیه می‌کنند برای جلوگیری از به سرقت رفتن رمز عبور و یا غیرفعال شدن تجهیز موردنظر، زمانی که از سیستم استفاده نمی‌کنید بلوتوث گوشی هوشمند خود را خاموش نگه‌دارید. همچنین به کاربران توصیه می‌شود برای بالا بردن امنیت این تجهیز در برابر حملات هکرها از کدهای عبور مناسب استفاده کرده و احراز هویت از طریق دو کاربر را برای سامانه خود تعریف کنند.

اداره حراست آموزشکده شهید یزدانپناه سنندج