صفحه‌کلیدهای آسیب‌پذیر

آیا صفحه‌کلیدهای بی‌سیم عامل افشای اطلاعات هستند؟

محققان امنیتی با انجام آزمایش‌های تکنیکی نشان داده‌اند، برخی از صفحه‌کلیدهای بی‌سیم متعلق به شرکت‌هایی همچون توشیبا و اچ‌پی قادر هستند اطلاعات کاربران را در معرض خطر قرار دهند.

اگر از یک صفحه‌کلید بی‌سیم ارزان قیمت استفاده می‌کنید، ممکن است در معرض یک حمله هکری که keysniffer نامیده می‌شود، قرار داشته باشید. حمله‌ای که قادر است به بهترین شکل ممکن اطلاعات شما را در معرض تهدید قرار داده و ربایش کند. آن‌گونه که شرکت امنیتی Bastille گزارش داده است، keysniffer یک آسیب‌پذیری بزرگ است که روی تعدادی از برندهای معروف و مدل‌هایی از صفحه‌کلیدهای بی‌سیم متعلق به شرکت‌های اچ‌پی، توشیبا، Kensington، Insignia، Radio Shock، General Electric و غیره قرار دارد.

مطلب پیشنهادی

خطر در کمین چاپ سه بعدی
هکرها ممکن است به چاپگرهای سه بعدی حمله کنند

KeySniffer به یک هکر اجازه می‌دهد از راه دور و از فاصله 250 فوتی به کلیدهایی که توسط کاربر فشار داده می‌شود، دسترسی داشته باشد. این داده‌ها در قالب یک متن شفاف قابل انتقال هستند. به‌طوری که گذرواژه، شماره کارت اعتباری و انواع دیگر اطلاعات حساس کاربران را به راحتی در معرض تهدید قرار می‌دهد. Bastille صفحه‌کلیدهای متعلق به 12 سازنده مختلف را مورد بررسی قرار داده و کشف کرده است که هشت مورد از آن‌ها قادر هستند اطلاعات کاربران را در معرض تهدید قرار دهند. در این میان شرکت Kensington وصله‌های مربوطه را عرضه کرده است و همچنین الگوریتم رمزنگاری AES را به‌طور گسترده برای صفحه‌کلیدهای این شرکت منتشر کرده است. اگر جزء آن گروه از کاربرانی هستید که از صفحه‌کلیدهای تحت آزمایش این شرکت استفاده می‌کنند، بهتر است به دنبال یک مدل دیگر باشید یا حداقل تهمیداتی در ارتباط با بلوتوث را لحاظ کنید. در دنیای واقعی رخنه‌های بسیاری وجود دارند که به اندازه کافی قدرتمند بوده و شما را به هدفی مناسب برای هکرها تبدیل می‌کنند؛ به‌طوری که هر روزه نگران از دست دادن اطلاعات شخصی خود باشید، در نتیجه بهتر است حداقل از این یک مورد خیال خود را آسوده کنید.

تاریخ انتشار:

09 مرداد 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3980