کشف آسیب پذیری خطرناک در ماژول های امنیتی سخت افزاری - دیجیاتو

حمید مقدسی | دوشنبه، ۲۰ خرداد ۱۳۹۸

دو محقق امنیتی به تازگی آسیب پذیری مهمی را کشف کرده اند که امکان بازیابی اطلاعات حساس ذخیره شده درون تجهیزات کامپیوتری خاص به نام «ماژول های امنیتی سخت افزاری» یا HSM را به مهاجمین می دهد.

ماژول های امنیتی سخت افزاری یا HSM قطعاتی هستند که از سازوکارهای رمزنگاری پیشرفته برای ذخیره سازی و استفاده از داده های حساس مثل کلیدهای دیجیتال، رمزهای عبور، پین کدها و دیگر اطلاعات مشابه استفاده می کنند. این قطعات معمولاً به شکل کارت های سخت افزاری، دستگاه های متصل به شبکه یا درایوهای USB عرضه می شوند.

دو نمونه HSM ساخت شرکت Gemalto

استفاده از HSM در مؤسسات مالی، نهادهای دولتی، دیتاسنترها، تأمین کنندگان خدمات کلاود و اپراتورهای مخابراتی رایج است. کیف پول های سخت افزاری ارزهای دیجیتال هم در واقع نوعی HSM به شمار می روند. حالا دو محقق امنیتی در کنفرانسی که هفته گذشته در فرانسه برگزار شد، چند آسیب پذیری را در HSM های ساخت یکی از برندهای معتبر افشا کرده اند.

احتمالاً این آسیب پذیری در محصولات شرکت Gemalto کشف شده است
طبق اطلاعات موجود، این آسیب پذیری ها به مهاجمین اجازه می دهند کنترل کامل HSM را از

راه دور در اختیار بگیرند. فرد مهاجم از این طریق به کلیدهای رمزنگاری و سطح دسترسی ادمین می رسد و حتی می تواند با دستکاری امضای دیجیتال فرمور، نسخه تغییر یافته از فرمور را روی HSM بارگذاری کند. بدین ترتیب حتی آپدیت های بعدی هم نمی تواند مشکل را رفع کند.

طبق گفته تیم امنیتی کریپتوسنس، این روش حمله کار سختی نیست و احتمال دارد دیگران هم تا به امروز حفره های امنیتی ماژول های امنیتی سخت افزاری را کشف کرده باشند. مهم ترین نگرانی محققین این است که هکرها با آپلود فرمور آلوده به درب پشتی (بک دور) مانع از رفع آسیب پذیری شوند. خلاصه روش هک ماژول های HSM توسط تیم متخصصین Ledger را می توانید از این لینک مطالعه کنید.

دیجیاتو