اینتل پس از ۹ سال، نقص امنیتی خطرناکی را در چیپ های سازمانی خود شناسایی کرد - دیجیاتو

حمید مقدسی | چهارشنبه، ۱۳ اردیبهشت ۱۳۹۶

اینتل به تازگی نوعی آسیب پذیری خاص در چیپ های ورک استیشن و سرورش را شناسایی کرده که می تواند دسترسی و کنترل کامل دستگاه را برای مهاجمین از راه دور میسر سازد. این باگ در فرمور «تکنولوژی مدیریت فعال» (AMT) فعال از نسخه 6 تا 11.6 وجود دارد.

ابزار مدیریتی AMT امکان احراز هویت کاربران را برای مدیریت دستگاه از راه دور میسر می سازد و در صورت دسترسی به درایورهای مناسب، قابلیت کنترل از راه دور دسکتاپ (ریموت دسکتاپ) را نیز در اختیار کاربر قرار می دهد. معمولاً این سامانه به رمز عبور نیاز دارد، اما آسیب پذیری مورد بحث به راحتی دور زدن مکانیسم امنیتی را ممکن ساخته و هر فردی با در اختیار داشتن یک «متاسپلویت» می تواند وارد سیستم شود.

صدها میلیون دستگاه کامپیوتر حساس سازمانی به این آسیب پذیری دچارند

شاید عجیب ترین نکته در مورد نقص فوق این است که حدود 9 سال ناشناخته باقی مانده بود، یعنی اینتل حدود یک دهه به فروش چیپ های آسیب پذیر می پرداخته و بنابراین صدها میلیون کامپیوتر در سرتاسر جهان در معرض خطر قرار گرفته اند. با توجه به اینکه بیشتر این چیپ ها در کامپیوترهای شرکتی به کار می روند، اطلاعات حساسی در دسترس مهاجمین قرار دارند.

اگرچه شرکت *SemiAccurate* مدعیست تمامی چیپ های مبتنی بر معماری Nehalem اینتل از نوامبر 2008 تا به امروز، یعنی حتی نسل جدید کیبی لیک هم به این مشکل دچارند، اما اینتل می گوید کامپیوترهای خانگی در معرض خطر نیستند.

به هر حال تنها راه غلبه بر این مشکل، آپدیت فرمور است که اینتل آن را منتشر ساخته، اما تولیدکنندگان مختلف باید آن را برای دستگاه های ساخت خودشان عرضه کنند و با توجه به حرکت لاک پشتی اکثر این شرکت ها، احتمالاً چندین هفته طول می کشد تا شاهد رفع کامل این آسیب پذیری باشیم.

ديجياتو