کشف یک آسیب پذیری دیگر در چیپ های اینتل: با ZombieLoad آشنا شوید - دیجیاتو

مریم موسوی | چهارشنبه، ۲۵ اردیبهشت ۱۳۹۸

شکاف امنیتی جدیدی که در پردازنده های اینتل کشف شده به هکرها امکان می دهد کلیه اطلاعاتی که پیشتر پردازنده به آنها دسترسی پیدا کرده را سرقت نمایند و متاسفانه این آسیب پذیری حتی سرورهای کلاود را نیز درگیر کرده و امکان سرقت اطلاعات از ویرچوال ماشین های اجرا شونده روی پی سی قربانی را هم فراهم می کند.

هنوز مشخص نیست حمله ای از طریق این آسیب پذیری که ZombieLoad نام گرفته توسط هکرها رخ داده یا نه اما خود آن را جمعی از محققان دانشگاه فناوری گریز کشف کردند و به اطلاع اینتل رساندند. اینتل هم در پاسخ به این اتفاق پچ مربوط به آسیب پذیری ZombieLoad را ارائه کرده هرچند در مرحله نخست شرکت های سازنده گوشی و سپس کاربران باید آن را روی گوشی های خود نصب کنند.

طبق گزارش تک کرانچ این نقص امنیتی تقریبا کلیه چیپ های تولیدی اینتل از سال ۲۰۱۱ را تحت تاثیر قرار داده است و آنطور که وایرد نوشته اپل و گوگل بلافاصله پچ های مربوط به آن را منتشر کردند و مایکروسافت نیز دقایقی پیش اقدام به این کار کرد.

اما برای آنکه هکرها از ZombieLoad استفاده کنند باید بتوانند کد مخرب را روی یک دستگاه اجرا

نمایند؛ در نتیجه همه در معرض خطر این آسیب پذیر قرار ندارند.

آسیب پذیری ZombieLoad را می توان جدیدترین حلقه در زنجیره شکاف های امنیتی چیپ های اینتل خواند که از فرایندی به نام اجرای زودهنگام (speculative execution) در اغلب پردازنده های مدرن بهره می گیرد. به لطف این امکان پردازنده ها به شکلی پیشگیرانه فرامین آینده را اجرا می کنند. اما آنطور که محققان نخستین بار در آسیب پذیری های ملت داون و اسپکتر متوجه شدند این فرایند حفره هایی را برای نفوذ هکرها ایجاد می کند.

پچ هایی که برای رفع این آسیب پذیری ها ارائه شده سرعت پردازنده ها را تا حدودی پایین آورد هرچند که باز هم امکان حمله هکرها وجود دارد. در واقع محققان باور دارند با وجود *اجرای زودهنگام* همچنان باید انتظار کشف آسیب پذیری های دیگری را داشت. اسپکتر و ملت داون دو آسیب پذیری نخست بودند و چند ماه بعد کارشناسان حوزه امنیت متوجه یک باگ دیگر شدند.

خوشبختانه تا به امروز این حملات پیامدها و اثرات ترسناکی که دانشمندان پیش بینی کرده بودند را در پی نداشته اند. البته پچ های زیادی هم برای رفع آنها ارائه شده است اما فرایند به کارگیری آنها آرام پیش رفته و همچنان خطر بروز یک حمله بسیار بزرگ با کمک این آسیب پذیری ها وجود دارد.

دیجیاتو