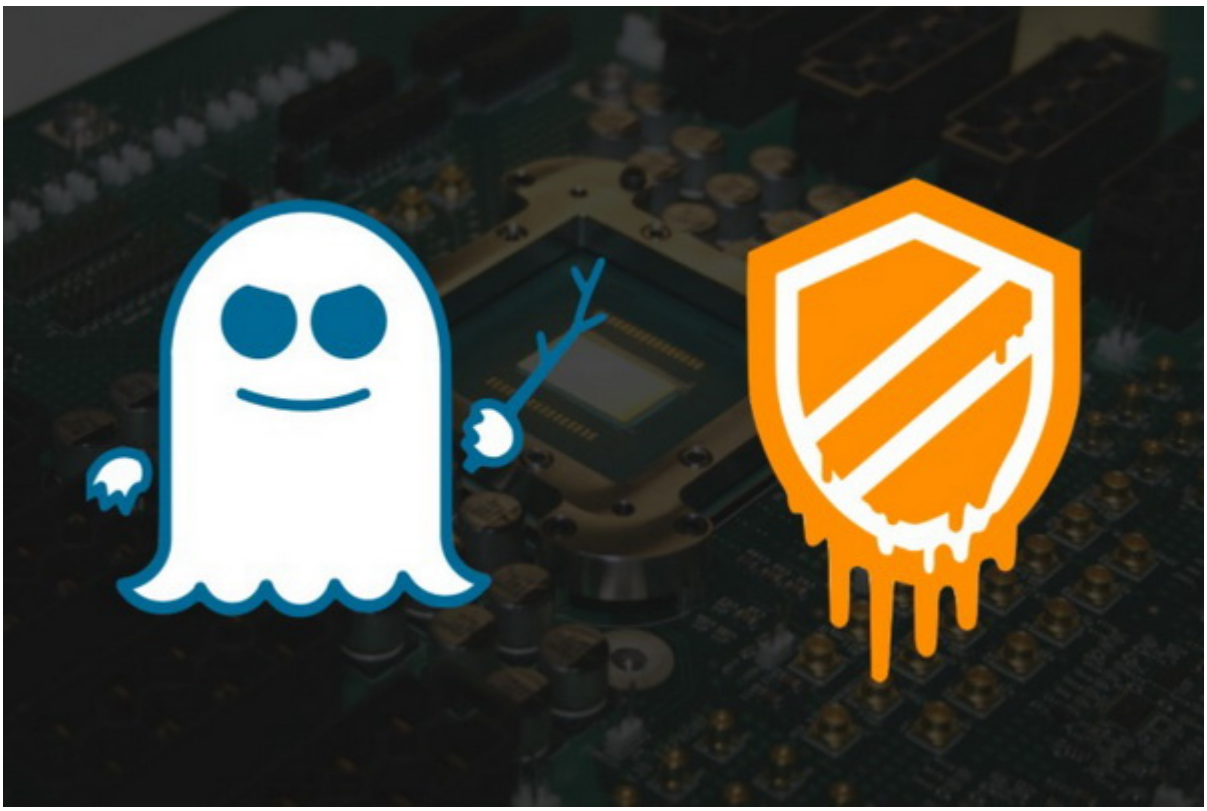
کشف ۷ آسیب پذیری جدید پردازنده مبتنی بر ملت داون و اسپکتر - دیجیاتو

علی باقرزاده | پنجشنبه، ۲۴ آبان ۱۳۹۷

ظاهراً دردسرهایی که در اثر آسیب پذیری های اسپکتر و ملت داون پیش می آیند تمامی ندارند و محققان از انواع جدید از حمله های مبتنی بر این دو حفره خبر داده اند.

اسپکتر و ملت داون آسیب پذیری هایی بودند که در حدود اوایل سال جاری میلادی خبر ساز شدند. این آسیب پذیری ها از نوعی طراحی در بسیاری از پردازنده های تولید شده توسط شرکت هایی از جمله اینتل و AMD یا طراحی شده توسط ARM در سال های اخیر سوء استفاده می کردند. هکرها با استفاده از آنها می توانستند به داده های کاربران دسترسی غیر مجاز پیدا کنند.

از بین آسیب پذیری هایی که به تازگی مطرح شده اند 5 مورد از نوع اسپکتر اولیه به شمار می روند و دو مورد دیگر از نوع ملت داون هستند. حمله جدید می تواند بر پردازنده های اینتل، AMD یا ARM تأثیر بگذارد.



به گفته محققان این آسیب پذیری هم از همان مکانیزم هایی ناشی می شود که در طراحی

بسیاری از پردازنده های برای پردازش داده ها مورد استفاده قرار می گیرد. یکی از این موارد، فرایند اجرای زود هنگام است. این فرایند که طراحی اولیه آن به سال 1995 باز می گردد امکان حدس زدن وظایف بعدی در پردازنده را فراهم می کند تا به این ترتیب برخی از پردازش ها سریع تر انجام شوند. اما از آنجایی که برخی از این پردازش ها که بدون استفاده می مانند، محافظت نمی شوند امکان استخراج اطلاعات احتمالاً مهم فراهم می شود.

اینتل اعلام کرده که می توان با روش هایی که برای رفع نسخه های قبلی ارائه شده بود جلوی حمله های جدید را هم گرفت. سخنگوی شرکت ARM هم پاسخ مشابهی داده اما هنوز پاسخی از سوی AMD دریافت نشده است.

اطلاعات دقیق مرتبط با این 7 روش حمله در سند کاملی منتشر شده است.

تماشا کنید: پلان؛ آشنایی با حفره های امنیتی اسپکتر و ملتداون در پردازنده ها

دیجیاتو