آسیب پذیری جدید اسپکتر هکرها را از دسترسی فیزیکی به سیستم بی نیاز می کند - دیجیاتو

یونس مرادی | یکشنبه، ۰۷ مرداد ۱۳۹۷

محققین «دانشگاه فناوری Graz» در اتریش از حمله سایبری جدیدی به نام NetSpectre خبر داده اند که بدون اجرای هیچ کدی در سیستم قربانی، داده ها از روی مموری به سرقت می برد.

حملات اسپکتر قبلی مستلزم دسترسی فیزیکی به کامپیوتر هدف و اجرای کدهای مخرب در آن هستند اما در این روش هکرها نیازی به این دسترسی ها ندارند. اساس این روش جدید نیست و بر چگونگی پیش بینی پردازنده از مسیر پردازش جاری تکیه می کند.

پردازنده های امروزی برای پردازش سریعتر پروسه ها از قابلیتی به نام اجرای زودهنگام بهره می برند. طی این فرایند بخشی از عملیات پردازشی آتی پیش بینی شده و به این طریق سرعت کار بالاتر می رود. مشکل این قابلیت از آنجا ناشی می شود که هکرها از طریق کدهای مخرب به اطلاعات دسترسی پیدا می کنند.

در این سناریو هکر باید به سیستم دسترسی داشته باشد یا حداقل قربانی بدافزارهای جاوا اسکریپت را روی سیستم دانلود کند. با این حال NetSpectre ویژگی متمایزی نسبت به دیگر حملات اسپکتر دارد و آن هم عدم نیاز به دسترسی فیزیکی یا دانلود کدها است.

در این روش هکر پورت های شبکه سیستم هدف را با کدهای مخرب بمباران کرده و برای دسترسی به داده های روی مموری، زمان پاسخ دهی را برآورد می کنند. خبر خوب اینجاست که در این روش انتقال داده ها با سرعت بسیار پایین ۶۰ بیت در ساعت صورت می گیرد اما اگر مهاجم برای دسترسی به یک کلید تنها چند بایت را لازم داشته باشد آنگاه مشکل جدی خواهد شد.

به گفته محققان اتریشی حمله NetSpectre از دو بخش تشکیل شده است. بخش اول ابزار نشت است که داده ها را از حافظه بیرون می کشد و بخش دوم هم ابزار مخابره ای است که وضعیت پردازنده را در شبکه نمایان می کند.

خوشبختانه این آسیب پذیری به وصله جدیدی نیاز ندارد و به گفته اینتل از طریق تکنیک های رفع اسپکتر و ملت داون برطرف می شود. این شرکت در پردازنده های جدید برای مقابله با مشکلاتی از این دست راه حل «بخش بندی» را در نظر گرفته که طی آن لایه اضافه ای بین اپلیکیشن های عادی و بخش سطح دسترسی کاربر قرار می گیرد.

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

[دیجیاتو]