گوگل از نقص امنیتی خطرناک پردازشگرهای گرافیکی آدرنو کوالکام پرده برداشت - دیجیاتو

محمد قریشی | سه شنبه، ۲۵ آذر ۱۳۹۹

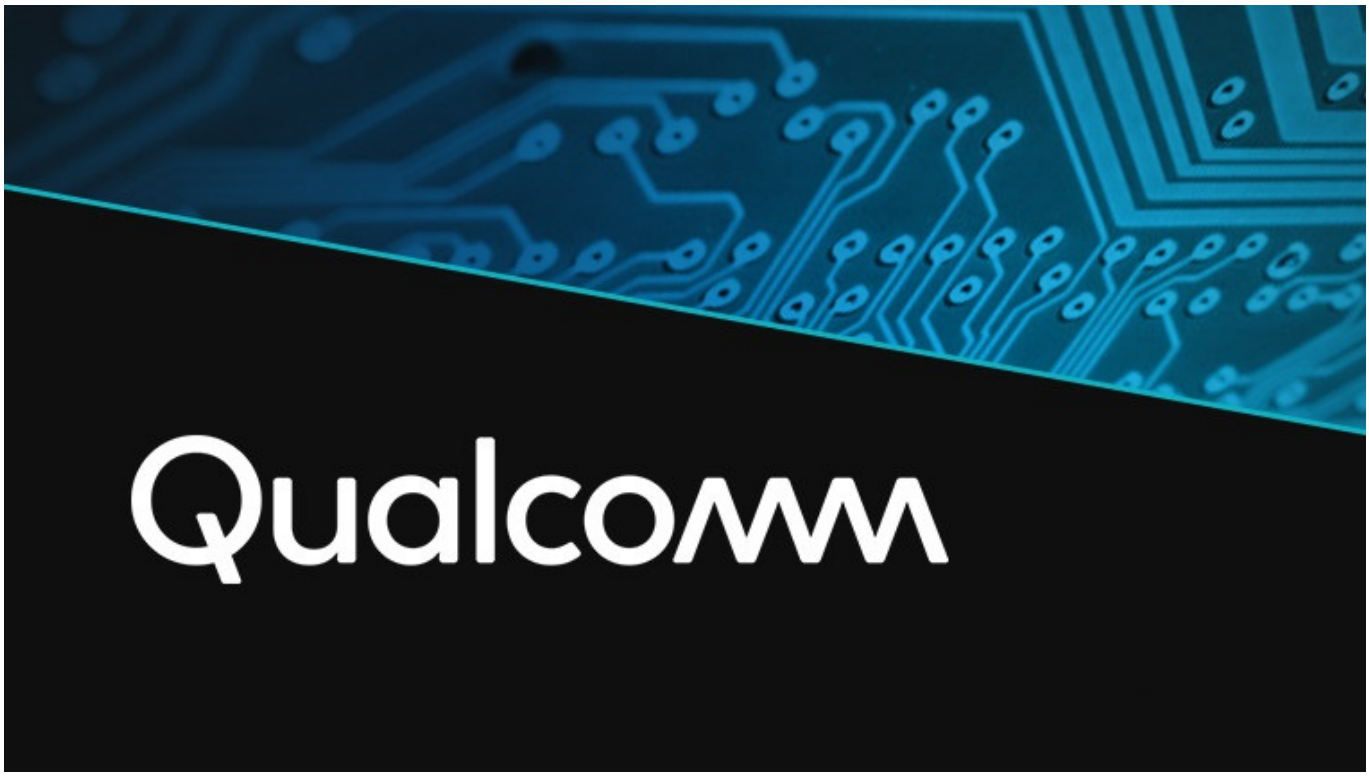
گوگل تحت «Project Zero» به دنبال کشف آسیب‌پذیری‌ها در محصولات خود و کمپانی‌های دیگر است که حالا نوبت به GPU آدرنو تراشه‌های کوالکام رسیده. گوگل به تازگی جزئیات این نقص امنیتی را منتشر کرده و البته کوالکام آن را برطرف کرده و باید راه‌حل آن را ارائه کند.

گوگل تحت پروژه خود مشکلات امنیتی را شناسایی می‌کند و به سازندگان آن‌ها اطلاعات می‌دهد. این کمپانی‌ها تا ۹۰ روز فرصت دارند این مشکلات را برطرف کنند و پس از این بازه زمانی، گوگل جزئیات آن‌ها را به صورت عمومی منتشر می‌کند.

تا به امروز این تیم آسیب‌پذیری‌های زیادی را در کرنل مک او اس، iOS و ویندوز ۱۰ اس شناسایی کرده و جدیدترین آن‌ها، یک نقص امنیتی جدی در واحد پردازش گرافیکی آدرنو در چیپ‌های اسنپدراگون کوالکام است. پس از پایان مهلت ۹۰ روزه، حالا شاهد انتشار جزئیات آن هستیم.

درایور GPU آدرنو یک ساختار خصوصی دستگاه را با هر توصیف‌کننده لایه پشتیبان کرنل گرافیکی (KGSL) پیوند می‌دهد که شامل جداول صفحه موردنیاز برای سوییچ متن می‌شود. این ساختار با فرایند آیدی (PID) مرتبط است که در هنگام فراخوانی می‌توان دوباره از آن توسط دیگر توصیف‌کنندگان KGSL در فرایندی یکسان استفاده کرد. چنین کاری عملکرد را بهبود می‌دهد.

زمانی که فورک‌های فرایند برای ایجاد یک فرایند فرزند (Child Process) فراخوانده می‌شوند، این فرایند ساختار خصوصی توصیف‌کننده KSGL که در ابتدا توسط فرایند والد (Parent Process) ایجاد شده را به ارث می‌برد و ساختار جدیدی تولید نمی‌کند. این موضوع باعث می‌شود که فرایند فرزند که می‌تواند یک مهاجم باشد، به نگاشت‌های بعدی GPU که توسط فرایند والد خلق می‌شوند، دسترسی پیدا کند و والد هم از آن بی‌اطلاع خواهد بود.



با یک حمله پیچیده روبه‌رو هستیم و به گفته تیم گوگل در یک سناریو در دنیای واقعی برای استفاده از این آسیب‌پذیری مهاجم باید یک لوپ از PID ایجاد کند و سپس آن را به موقع راه‌اندازی کرده یا به وسیله یک باگ سیستم را ریستارت کند. در ادامه این اکسپلویت سعی می‌کند محتوای GPU قربانی را بازیابی کند.

این مشکل در تاریخ ۲۵ شهریور ماه به کوالکام اطلاع داده شد و حالا مهلت ۹۰ روزه به پایان رسیده. کوالکام در تاریخ ۱۷ آذر این مشکل را برطرف و اطلاعات آن را به صورت خصوصی با تولیدکنندگان به اشتراک گذاشته. این کمپانی در صحبت با تیم گوگل از انتشار عمومی جزئیات این آسیب‌پذیری در ژانویه ۲۰۲۱ خبر داده است.

حالا که چنین مشکلی به صورت عمومی اعلام شده، کوالکام باید هرچه سریعتر راه‌حل این مشکل را ارائه کند تا هکرها با استفاده از این آسیب‌پذیری نتوانند به دستگاه‌ها حمله کنند.

دیجیاتو