بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

وصله آسیب‌پذیری‌های موجود در دستگاه‌های اندروید

گزارش آسیب‌پذیری

فهرست مطالب

۱ وصله آسیب‌پذیری‌های موجود در دستگاه‌های اندروید

گوگل و Qualcomm آسیب‌پذیری‌های قابل توجهی را در به‌روزرسانی‌های ژوئن وصله کردند. گوگل دو آسیب‌پذیری بحرانی که باعث اجرای کد از راه دور در دستگاه‌های موبایل اندروید می‌شوند را در به‌روزرسانی اخیر خود وصله کرد. این دو آسیب‌پذیری بحرانی (CVE-2020-0117 و CVE-2020-8597) در سیستم اندروید وجود داشته و به یک مهاجم از راه دور امکان می‌دهد با استفاده از یک انتقال خاص، کد دلخواه خود را در چارچوب یک فرآیند ممتاز اجرا کند. این آسیب‌پذیری‌ها نسخه‌های اندروید ۸ تا ۱۰ را تحت تأثیر خود قرار می‌دهند.

طبق گزارشات منتشر شده از این آسیب‌پذیری‌ها می‌توان از روش‌های متفاوتی مانند ایمیل، مرورگر وب و MMS در حین پردازش فایل‌های چند رسانه‌ای بهره‌برداری کرد. بر اساس دسترسی‌های اختصاص داده شده به برنامه، مهاجم می‌تواند برنامه‌هایی را نصب، داده‌ها را مشاهده، تغییر یا حذف کند یا حساب‌های کاربری با دسترسی بالا ایجاد کند.

آسیب‌پذیری‌های دیگری که وجود دارند، دو آسیب‌پذیری افشای اطلاعات با شدت بالاست (CVE-2020-0116 و CVE-2020-0119) که بر اندروید ۱۰ تأثیر می‌گذارد و گوگل جزییات فنی برای آن‌ها ارائه نداده است.

به‌روزرسانی‌های امنیتی ژوئن همچنین آسیب‌پذیری‌های موجود در Android Framework را رفع کرده است. این آسیب‌پذیری‌ها شامل آسیب‌پذیری افزایش دسترسی (EoP) با شناسه CVE-2020-0114 در اندروید ۱۰ است که ممکن است باعث فعال‌سازی یک برنامه مخرب محلی جهت دور زدن نیازمندی‌های تعامل کاربری و به دست آوردن دسترسی‌های اضافی شود.

آسیب‌پذیری‌های CVE-2020-0115، مشکل EoP در اندروید ۸ تا ۱۰ و CVE-2020-0121، مشکل افشای اطلاعات در اندروید ۱۰ نیز وصله شد. دو وصله نیز برای آسیب‌پذیری‌های Android Media Framework وجود دارد، شامل آسیب‌پذیری CVE-2020-0118 که یک برنامه مخرب محلی را جهت دور زدن نیازمندی‌های تعامل کاربری و به دست آوردن دسترسی‌های اضافی در اندروید ۱۰ فعال می‌کند و آسیب‌پذیری CVE-2020-0113 نیز یک آسیب‌پذیری افشای اطلاعات است که بر اندروید ۹ و ۱۰ تأثیر می‌گذارد.

سه آسیب‌پذیری امنیتی با شدت بالا نیز در اجزای هسته اندروید وجود دارند. شدیدترین آن‌ها (CVE-2020-8647)، به یک مهاجم محلی امکان می‌دهد با استفاده از یک برنامه خاص کد دلخواه خود را در در چارچوب یک فرآیند ممتاز اجرا کند، دو آسیب‌پذیری دیگر (CVE-2020-8648 و CVE-2020-8428) نیز با شدت بالا محاسبه شده‌اند. گوگل همچنین مشاوره‌های مربوط به دو آسیب‌پذیری قدیمی را به روز کرد: CVE-2019-2219 که بر Framework در اندروید ۸ تا ۱۰ وجود داشته و به یک برنامه مخرب محلی امکان می‌دهد

محافظت‌های سیستم‌عامل که باعث جداسازی داده‌های برنامه از سایر برنامه‌ها می‌شود را دور بزند و آسیب‌پذیری EoP در سیستم (CVE-2019-9460) که به مهاجم از راه دور امکان می‌دهد نیازمندی‌های تعامل کاربری را دور زده و دسترسی‌های اضافی به دست آورد. در به‌روزرسانی‌های ماه گذشته اندروید، ۳۹ آسیب‌پذیری رفع شده است.

همچنین در هفته گذشته وصله‌هایی برای رفع آسیب‌پذیری‌های متعدد موجود در بخش‌های Qualcomm مورد استفاده در اندروید منتشر شد. دو مورد از این آسیب‌پذیری‌ها بحرانی گزارش شده و می‌تواند از راه دور بهره‌برداری شود. این آسیب‌پذیری‌ها هر دو در قسمت data-modem تراشه‌های تلفن همراه Qualcomm وجود دارند.

آسیب‌پذیری با شناسه CVE-2019-14073 نیز باعث می‌شود بافرهای سیستم بدون بررسی اندازه ورودی در data-modem، کپی شوند. کپی کردن پیام‌های RTCP در بافر خروجی بدون بررسی اندازه بافر مقصد می‌تواند باعث سرریز بافر از راه دور در هنگام پردازش داده‌های بزرگ یا پیام‌های بازخورد غیر استاندارد شود.

۲ مراجع

[1] https://threatpost.com/two-critical-android-bugs-rce/156216/