بسمه تعالی

به‌روزرسانی ماه ژوئیه‌ی اندروید و رفع ۹ آسیب‌پذیری بحرانی

شرکت گوگل وصله‌هایی برای سیستم‌عامل اندروید منتشر کرد تا به‌طور کلی، ۳۳ آسیب‌پذیری که شامل ۹ آسیب‌پذیری بحرانی است، رفع کند.

این آسیب‌پذیری‌ها بر روی اجزای مختلف اندروید ازجمله سیستم‌عامل اندروید، چارچوب، کتابخانه، چارچوب رسانه‌ای و همچنین مؤلفه‌های کوالکام تأثیر می‌گذارند.

سه مورد از آسیب‌پذیری‌های بحرانی این ماه، در چارچوب رسانه‌ی اندروید قرار دارند که به یک مهاجم اجازه می‌دهند تا از راه دور و با استفاده از یک فایل خاص طراحی‌شده، کد دلخواه را در چارچوب یک فرایند خاص، اجرا کند.

CVE	نوع آسیب‌پذیری	شدت آسیب‌پذیری	نسخه‌های به‌روزشده
CVE-2019-2106	اجرای کد از راه دور	بحرانی	۷ به بالا
CVE-2019-2107	اجرای کد از راه دور	بحرانی	۷ به بالا
CVE-2019-2109	اجرای کد از راه دور	بحرانی	۷ به بالا

از میان شش آسیب‌پذیری بحرانی دیگر، یکی از آن‌ها بر روی سیستم اندروید تأثیرمی‌گذارد.

CVE	نوع آسیب‌پذیری	شدت آسیب‌پذیری	نسخه‌های به‌روزشده
CVE-2019-2111	اجرای کد از راه دور	بحرانی	۹

دو آسیب‌پذیری بحرانی دیگر در مؤلفه‌های "DSP-Services" و "Kernel" و سه مورد در مؤلفه‌ی متن بسته‌ی کوالکام وجود دارند.

CVE	نوع آسیب‌پذیری	شدت آسیب‌پذیری	مؤلفه
CVE-2019-2308	عدم امکان طبقه‌بندی	بحرانی	DSP_Services
CVE-2019-2330	عدم امکان طبقه‌بندی	بحرانی	Kernel
CVE-2019-2254	عدم امکان طبقه‌بندی	بحرانی	مؤلفه‌ی متن بسته
CVE-2019-2322	عدم امکان طبقه‌بندی	بحرانی	مؤلفه‌ی متن بسته
CVE-2019-2327	عدم امکان طبقه‌بندی	بحرانی	مؤلفه‌ی متن بسته

یک خطای دارای شدت بالا نیز در کتابخانه‌ی اندروید وجود دارد که می‌تواند به مهاجم، اجازه‌ی اجرای کد از راه دور دهد.

CVE	نوع آسیب‌پذیری	شدت آسیب‌پذیری	نسخه‌های به‌روزشده
CVE-2019-2105	اجرای کد از راه دور	بالا	۷ به بالا

علاوه‌براین، یک خطای شدید در چارچوب اندروید وجود دارد که می‌تواند به یک برنامه‌ی مخرب نصب‌شده، اجازه‌ی دورزدن الزامات تعامل کاربر را بدهد تا بتواند به مجوزهای اضافی دسترسی پیدا کند.

CVE	نوع آسیب‌پذیری	شدت آسیب‌پذیری	نسخه‌های به‌روزشده
CVE-2019-2104	افشای اطلاعات	بالا	۸.۰ ۸.۱ ۹

شش آسیب‌پذیری شدید نیز در مؤلفه‌های کوالکام رفع شدند که در میزبان WLAN (CVE-2019-2276، CVE-2019-2307)، درایور WLAN (CVE-2019-2305)، HLOS (CVE-2019-2278)و صدا (CVE-2019-2326، CVE-2019-2328) وجود دارند.

وصله‌ی امنیتی اندروید علاوه بر انتشار وصله‌هایی برای آسیب‌پذیری‌های امنیتی، شامل رفع مشکلات مختلف در برخی از نسخه‌های پشتیبانی‌شده از دستگاه‌های پیکسل است.

کاربران گوشی‌های هوشمند پیکسل به‌زودی به‌روزرسانی ماه ژوئیه را دریافت خواهند کرد و کاربران دیگر دستگاه‌ها باید به محض انتشار وصله‌ها توسط تولیدکنندگان، آخرین نسخه‌ی امنیتی اندروید را دانلود کنند تا از دستگاه‌های اندرویدی خود در برابر هرگونه حمله‌ی احتمالی محافظت نمایند.