بسمه تعالی

سوءاستفاده از سرویس MediaProjection در اندروید برای دریافت صفحه‌ی نمایش و ضبط صدای سیستم

گوشی‌های هوشمند اندرویدی که Lolipop، Marshmallow و Nougat را اجرا می‌کنند، نسبت به حمله‌ای که از سرویس MediaProjection سوءاستفاده می‌کند، آسیب‌پذیر هستند. MediaProjection یک سرویس اندروید است که قادر به دریافت محتویات صفحه‌ی نمایش و ضبط صدای سیستم است.

این سرویس از زمان آغاز فعالیت خود، در اندروید وجود داشته است. برنامه‌های کاربردی برای استفاده از این سرویس، نیاز به دسترسی به مجوز سطح ریشه دارند و باید با کلیدهای دستگاه امضا شوند. همین امر، MediaProjection را به برنامه‌های سطح سیستم که توسط OEM–های (Original Equipment Manufacture) تحت اندروید توسعه‌یافته‌اند، محدود می‌کند.

طبق آمار به‌دست‌آمده از توزیع این دستگاه‌ها در بازار، ۷۷/۵ درصد (سه‌چهارم) از تمام دستگاه‌های اندروید، تحت تأثیر این آسیب‌پذیری قرارگرفته‌اند.

با انتشار Android Lolipop (5.0)، گوگل این سرویس را بدون نیاز به مجوزی که برنامه‌های کاربردی پیش از نصب از کاربر درخواست می‌کنند، در اندورید قرار داد. آگاهی از همین موضوع باعث شد تا برنامه‌ها از طریق یک «تماس عمدی»، دسترسی به این سرویس سیستمی را درخواست کنند. این تماس عمدی و استفاده از سرویس، یک پنجره‌ی پاپ‌آپ SystemUI را به کاربر نشان می‌دهد که هنگام گرفتن عکس از صفحه و ضبط صدای سیستم توسط برنامه، به کاربر هشدار می‌داد.

در اوایل زمستان سال گذشته (۲۰۱۶)، محققان امنیتی آزمایشگاه MWR کشف کردند که مهاجم می‌تواند زمان ظاهر شدن پنجره SystemUI را شناسایی کند. با دانستن این زمان، مهاجمان می‌توانند پنجره‌ی دلخواهی را بر روی آن نشان دهند و متن آن را با پیام دیگری مخفی کنند.

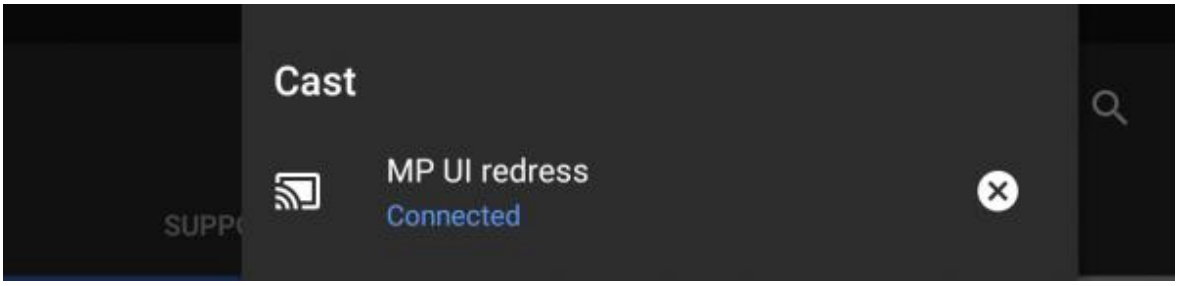
این روش به نام ضربه–سرقت شناخته‌شده است و چندین سال است که توسط توسعه‌دهندگان بدافزار اندروید مورداستفاده قرار می‌گیرد. در این روش، مهاجمان ضربات کاربر بر روی صفحه را به سرقت می‌برند و از آن‌ها برای رسیدن به هدف موردنظر خود استفاده می‌کنند.

گروه تحقیقاتی MWR در گزارشی توضیح داد که علت اصلی این آسیب‌پذیری این واقعیت است که نسخه‌های اندرویدی که تحت تأثیر آن قرار می‌گیرند، قادر به تشخیص پنجره‌های SystemUI پنهان‌شده نیستند. همین امر به مهاجم اجازه می‌دهد تا برنامه‌ای کاربردی ایجاد کند که می‌تواند یک هم‌پوشانی بر روی پاپ‌آپ SystemUI تولید کند. این هم‌پوشانی منجر به افزایش مجوزهای برنامه می‌شود و اجازه‌ی دریافت صفحه‌ی نمایش کاربر را به مهاجم می‌دهد.

علاوه‌براین، پاپ‌آپ SystemUI تنها مکانیزم کنترل دسترسی است که از سوءاستفاده از سرویس MediaProjection جلوگیری می‌کند. مهاجم می‌تواند به‌طور بی‌رویه از این مکانیزم، با به سرقت بردن ضربات این پاپ‌آپ و به‌کارگیری روش‌های عمومی شناخته‌شده، استفاده کند تا برنامه‌ی کاربردی خود را قادر به ضبط صفحه‌ی نمایش کاربر کند.

گوگل این آسیب‌پذیری را در پاییز امسال در سیستم‌عامل اندروید با انتشار Android Oreo (8.0) برطرف کرده است؛ اما نسخه‌های قدیمی‌تر اندروید همچنان آسیب‌پذیر هستند.

محققان تأکید کردند که حمله‌ای که از این نقص سوءاستفاده می‌کند، کاملاً غیرقابل‌شناسایی نیست. هنگامی‌که یک برنامه‌ی کاربردی، دسترسی به سرویس MediaProjection را به‌دست می‌آورد، یک نمایش مجازی ایجاد می‌کند که آیکون Screencast را در نوار اعلان فعال می‌کند (شکل ۱).



شکل ۱ نمایش آیکون Screencast در نوار اعلان

هنوز مشخص نیست که آیا گوگل قصد دارد این آسیب‌پذیری را نیز برای نسخه‌های قدیمی‌تر آسیب‌پذیر اندروید حل کند یا خیر، به همین دلیل کاربران باید دستگاه‌های خود را به‌روز کنند.

MWR همچنین راه‌حلی برای توسعه‌دهندگان نرم‌افزار اندروید ارایه داده است که می‌تواند با تنظیم پارامتر طرح FLAG_SECURE از طریق WindowManager این مسئله را حل کند. این راه‌حل اطمینان می‌دهد که محتوای پنجره‌های برنامه‌های کاربردی، امن محسوب می‌شوند و مانع از نمایش آن در تصاویر یا مشاهده در نمایش‌های ناامن می‌شود.