بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

گزارش آسیب پذیری Android

گزارش خبری

شناسه سند ..... Android_Vulnerability_Report

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۴۰۲/۰۴/۱۷

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ شرح آسیب‌پذیری

گوگل برای ماه جولای، ۴۶ آسیب‌پذیری را در اندروید اصلاح کرده است. ۲ مورد دارای شدت بحرانی،یک مورد با شدت متوسط و بقیه موارد دارای شدت بالا هستند. ۳ مورد از این آسیب‌پذیری ها هم زیرودی است که قبلا در حملاتی مورد استفاده قرار گرفته است.

آسیب پذیری بخش Framework :

شدیدترین آسیب‌پذیری در این بخش می‌تواند منجر به افزایش امتیاز بدون نیاز به تعامل کاربر و امتیاز اجرایی اضافی می‌شود.

CVE	نوع	شدت	**نسخه‌های به‌روز شده AOSP**
CVE-2023-20918	EoP	High	11, 12, 12L, 13
CVE-2023-20942	EoP	High	12, 12L, 13
CVE-2023-21145	EoP	High	11, 12, 12L, 13
CVE-2023-21245	EoP	High	11, 12, 12L, 13
CVE-2023-21251	EoP	High	11, 12, 12L, 13
CVE-2023-21254	EoP	High	13
CVE-2023-21257	EoP	High	13
CVE-2023-21262	EoP	High	12, 12L, 13
CVE-2023-21238	ID	High	11, 12, 12L, 13
CVE-2023-21239	ID	High	12, 12L, 13
CVE-2023-21249	ID	High	13
CVE-2023-21087	DoS	High	**11, 12, 12L, 13**

آسیب پذیری بخش System :

شدیدترین آسیب‌پذیری در این بخش می‌تواند منجر به اجرای کد از راه دور و نیازی به تعامل کاربر نیست.در نهایت باعث امتیازات اجرایی اضافی می‌شود.

CVE	نوع	شدت	نسخه‌های به‌روز شده AOSP
CVE-2023-21250	RCE	Critical	11, 12, 12L, 13
CVE-2023-2136	RCE	High	۱۳
CVE-2023-21241	EoP	High	11, 12, 12L
CVE-2023-21246	EoP	High	11, 12
CVE-2023-21247	EoP	High	11, 12, 12L, 13
CVE-2023-21248	EoP	High	11, 12, 12L, 13
CVE-2023-21256	ID	High	11, 12, 12L, 13
CVE-2023-21261	ID	High	11, 12, 12L, 13
CVE-2023-20910	ID	High	11, 12, 12L, 13
CVE-2023-21240	ID	High	12L, 13
CVE-2023-21243	DOS	High	11, 12, 12L, 13

گوگل بیان کرده است که نشانه هایی وجود دارد که آسیب پذیری CVE-2023-2136 بصورت محدود و هدفمند مورد اکسپلویت قرار گرفته است. آسیب پذیری از نوع integer overflow در Skia است و شدت بحرانی و امتیاز ۹,۶ دارد. Skia یک کتابخانه گرافیکی متن باز چند پلتفرمی گوگل است که در کروم هم استفاده می‌شود، که در اواخر فروردین در کروم اصلاح شده بود.

آسیب پذیری مولفه های ARM :

این آسیب‌پذیری‌ها بر اجزای Arm تأثیر می‌گذارند و جزئیات بیشتر مستقیماً از شرکت Arm در دسترس است. ارزیابی شدت این مسائل نیز به صورت مستقیم توسط Arm ارائه می‌شود.

CVE	زیرمجموعه	شدت
CVE-2021-29256	Mali	**High**
CVE-2022-28350	Mali	**High**
CVE-2023-28147	Mali	**High**
CVE-2023-26083	Mali	**Moderate**

گوگل بیان کرده است که نشانه هایی وجود دارد که آسیب پذیری های CVE-2023-26083 و CVE-2021-29256 بصورت محدود و هدفمند مورد اکسپلویت قرار گرفته‌اند.

آسیب پذیری CVE-2023-26083 یک آسیب پذیری نشت حافظه با شدت متوسط است. آسیب پذیری در Arm Mali GPU مرتبط با چیپ‌های Bifrost و Avalon و Valhall رخ میدهد. از آسیب پذیری در یک زنجیره اکسپلویت، در دسامبر ۲۰۲۲ برای استقرار جاسوس افزار تجاری در دستگاههای سامسونگ استفاده شده است.

آسیب پذیری CVE-2021-29256 امکان افشای اطلاعات و افزایش امتیاز به کاربر root رو می‌دهد و دارای شدت بالا و امتیاز ۸,۸ است. آسیب پذیری روی نسخه های خاصی از درایورهای Midgard Arm Mali GPU و Bifrost تاثیر می‌گذارد.

.

آسیب پذیری بخش Imagination Technologies :

این آسیب‌پذیری روی مولفه های Imagination Technologies تاثیر گذار است و شدت و جزییات آن را کمپانی Imagination Technologies ارائه می‌دهد.

شدت	زیرمجموعه	CVE
High	PowerVR-GPU	CVE-2021-0948

آسیب پذیری های سیستم بروزرسانی Google Play:

این آسیب‌پذیری‌ها روی مولفه های Project Mainline تاثیر می‌گذارد.

شدت	زیرمجموعه	CVE
High	WiFi	CVE-2023-20910
High	WiFi	CVE-2023-21240
High	WiFi	CVE-2023-21243

آسیب پذیری های کرنل:

شدیدترین آسیب پذیری ها در این بخش منجر به افزایش امتیاز محلی در کرنل، بدون نیاز به تعامل کاربر و امتیازات اجرایی اضافی می‌شود.

نوع	شدت	زیرمجموعه	CVE
EoP	High	MemoryManagement	CVE-2022-42703
EoP	High	Binder	CVE-2023-21255

آسیب پذیری های مولفه های کرنل :

در این بخش، شدیدترین آسیب پذیری ها منجر به افزایش امتیاز محلی، بدون نیاز به تعامل کاربر و امتیازات اجرایی اضافی می‌شود.

نوع	شدت	زیرمجموعه	CVE
EoP	High	HID	CVE-2023-25012

آسیب پذیری های MediaTek :

این آسیب پذیری ها روی مولفه های MediaTek تاثیر گذار هستند و شدت و جزییات آنها را کمپانی MediaTek ارائه می‌دهد.

شدت	زیرمجموعه	CVE
High	keyinstall	CVE-2023-20754
High	keyinstall	CVE-2023-20755

آسیب پذیری بخش Qualcomm :

این آسیب پذیری‌ها روی مولفه های Qualcomm تاثیر می‌گذارد و شدت و جزییات ان را کمپانی Qualcomm ارائه میدهد.

شدت	زیرمجموعه	CVE
High	Audio	CVE-2023-21672
High	WLAN	CVE-2023-22386
High	Kernel	CVE-2023-22387
High	WLAN	CVE-2023-24851
High	WLAN	CVE-2023-24854
High	WLAN	CVE-2023-28541
High	WLAN	CVE-2023-28542

آسیب پذیری بخش Qualcomm closed-source :

این آسیب‌پذیری‌ها روی مولفه های Qualcomm closed-source تاثیر گذار است و شدت و جزییات آن توسط کمپانی Qualcomm ارائه می‌شود.

CVE	زیرمجموعه	شدت
CVE-2023-21629	Closed-source component	**Critical**
CVE-2023-21631	Closed-source component	**High**
CVE-2023-22667	Closed-source component	**High**

۲ مراجع

https://source.android.com/docs/security/bulletin/2023-07-01