بسمه‌تعالی

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 آسیب‌پذیری Android

گزارش فنی

شناسه سند ..... Android_Vulnerability_Report
نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۳/۲۷
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 ۱
۲ مراجع ۳

۱ شرح آسیب‌پذیری

گوگل برای ماه ژوئن، ۵۶ آسیب‌پذیری را در اندروید اصلاح کرده است. ۵ مورد دارای شدت بحرانی و بقیه موارد دارای شدت بالا هستند. یکی از این آسیب‌پذیری ها هم زیرودی است که از دسامبر ۲۰۲۲ (آذر ۱۴۰۱) در حملاتی مورد استفاده قرار گرفته است.

آسیب پذیری بخش Framework :

شدیدترین آسیب‌پذیری در این بخش می‌تواند منجر به اجرای کد از راه دور با عدم نیاز به مجوزهای اجرای اضافی شود. برای بهره‌برداری از این آسیب‌پذیری، نیاز به تعامل کاربر است.

CVE	نوع	شدت	نسخه‌های به‌روز شده AOSP
CVE-2023-21127	RCE	Critical	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21126	EoP	High	۱۳
CVE-2023-21128	EoP	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21129	EoP	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21131	EoP	High	۱۳
CVE-2023-21139	EoP	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21105	ID	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21136	DoS	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21137	DoS	High	۱۲ ,۱۲ ,۱۱L, 13
CVE-2023-21143	DoS	High	۱۲ ,۱۲ ,۱۱L, 13

آسیب پذیری بخش System :

شدیدترین آسیب‌پذیری در این بخش می‌تواند منجر به اجرای کد از راه دور از طریق بلوتوث شود، در صورتی که پشتیبانی HFP فعال باشد ، نیازی به مجوزهای اجرای اضافی ندارد. برای بهره‌برداری از این آسیب‌پذیری، نیازی به تعامل کاربر نیست.

CVE	نوع	شدت	نسخه‌های به‌روز شده AOSP
CVE-2023-21108	RCE	Critical	11, 12, 12L, 13
CVE-2023-21130	RCE	Critical	۱۳
CVE-2023-21115	EoP	High	11, 12, 12L
CVE-2023-21121	EoP	High	11, 12
CVE-2023-21122	EoP	High	11, 12, 12L, 13
CVE-2023-21123	EoP	High	11, 12, 12L, 13
CVE-2023-21124	EoP	High	11, 12, 12L, 13
CVE-2023-21135	EoP	High	11, 12, 12L, 13
CVE-2023-21138	EoP	High	11, 12, 12L, 13
CVE-2023-21095	ID	High	12L, 13
CVE-2023-21141	ID	High	11, 12, 12L, 13
CVE-2023-21142	ID	High	11, 12, 12L, 13
CVE-2023-21144	DoS	High	11, 12, 12L, 13

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-2022-22706	Mali	**Critical**
CVE-2022-28349	Mali	**Critical**
CVE-2022-46781	Mali	**High**

به گفته گروه تحلیل تهدیدات گوگل (TAG)، آسیب‌پذیری به شناسه CVE-2022-22706 در یک جاسوس افزار ، برای هدف قرار دادن کاربران گوشی های سامسونگ مورد استفاده قرار گرفته است. این آسیب پذیری که امتیاز ۷,۸ از ۱۰ را دارد به کاربران غیرمجاز امکان دسترسی "نوشتن"، به صفحات حافظه "فقط خواندنی" رو می‌دهد. به گفته ARM این آسیب پذیری روی محصولات زیر تاثیر گذار است:

Midgard GPU Kernel Driver: All versions from r26p0 – r31p0
Bifrost GPU Kernel Driver: All versions from r0p0 – r35p0
Valhall GPU Kernel Driver: All versions from r19p0 – r35p0

شرکت سامسونگ در بروزرسانی ماه مه، به این آسیب پذیری نیز اشاره کرده بود.

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.

CVE	زیرمجموعه	شدت
CVE-2021-0701	PowerVR-GPU	**High**
CVE-2021-0945	PowerVR-GPU	**High**

آسیب پذیری بخش Unisoc :

این آسیب‌پذیری‌ها روی مولفه های Unisoc تاثیر می‌گذارد و شدت و جزییات آن را کمپانی Unisoc ارائه میدهد.

CVE	زیرمجموعه	شدت
CVE-2022-48390	Android	**High**
CVE-2022-48392	Android	**High**
CVE-2022-48438	Kernel/Android	**High**
CVE-2022-48391	Android	**High**

آسیب پذیری بخش Widevine DRM:

این آسیب‌پذیری‌ها روی مولفه های Widevine DRM تاثیر گذار است و شدت و جزییات آن را کمپانی Widevine DRM ارائه میدهد.

CVE	زیرمجموعه	شدت
CVE-2023-21101	widevine	**High**
CVE-2023-21120	Hardware DRM	**High**

آسیب پذیری بخش Qualcomm :

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

CVE	زیرمجموعه	شدت
CVE-2022-33292	Kernel	**High**
CVE-2023-21656	WLAN	**High**
CVE-2023-21657	Audio	**High**
CVE-2023-21669	WLAN	**High**
CVE-2023-21670	Display	**High**

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-2022-33257	Closed-source component	**Critical**
CVE-2022-40529	Closed-source component	**Critical**
CVE-2022-22060	Closed-source component	**High**
CVE-2022-33251	Closed-source component	**High**
CVE-2022-33264	Closed-source component	**High**
CVE-2022-40516	Closed-source component	**High**
CVE-2022-40517	Closed-source component	**High**
CVE-2022-40520	Closed-source component	**High**
CVE-2022-40521	Closed-source component	**High**
CVE-2022-40523	Closed-source component	**High**
CVE-2022-40533	Closed-source component	**High**
CVE-2022-40536	Closed-source component	**High**
CVE-2022-40538	Closed-source component	**High**
CVE-2023-21628	Closed-source component	**High**
CVE-2023-21658	Closed-source component	**High**
CVE-2023-21659	Closed-source component	**High**
CVE-2023-21661	Closed-source component	**High**

۲ مراجع

https://source.android.com/docs/security/bulletin/2023-06-01