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 فنی آسیب پذیری Android

گزارش آسیب پذیری Android

شناسه سند ..... Android-Vulnerability-report-
نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۸/۲۲
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

گوگل برای ماه نوامبر، ۳۹ آسیب پذیری را در اندروید اصلاح کرده است. بیشتر آسیب پذیری ها شدت بالا دارند به غیر از ۵ مورد که شدت بحرانی دارند. گوگل در بروزرسانی این ماه، مواردی رو به‌عنوان زیرودی مشخص نکرده است. علاوه بر بروزرسانی و اصلاح آسیب پذیری‌ها، گوگل یک ویژگی امنیتی جدید را هم برای برنامه های VPN فعال کرده است.

۱-۱ چند نکته مهم در خصوص بروزرسانی

- گوگل جزییات زیادی در خصوص آسیب پذیری ها ،منتشر نمی‌کند تا کاربران فرصت کافی، برای بروزرسانی و ایمن کردن دستگاه داشته باشند. اگر از اندروید ۱۰ و پایین‌تر استفاده می‌کنید، به دلیل اینکه این نسخه ها، قدیمی شده‌اند ، دیگر توسط گوگل پشتیبانی نمی‌شوند. بنابراین این بروزرسانی‌ها برای دستگاه اعمال نمی‌شود. برای بروزرسانی می‌توانید از روش های زیر استفاده کنید:

  Settings → System → System Update → Check for updates

  Settings → Security&Privacy → Updates → Security update

- اگر از نسخه های ۱۰ و پایین‌تر استفاده می‌کنید، می‌توانید از توزیع‌های Third-Party Android مانند LineageOSاستفاده کنید .نوع آسیب پذیری‌ها را می‌توانید در زیر مشاهده کنید:

  - RCE مشخص کننده آسیب پذیری های اجرای کد از راه دور
  - EoP مشخص کننده آسیب پذیری های افزایش امتیاز
  - ID مشخص کننده آسیب پذیری های افشای اطلاعات
  - DoS مشخص کننده آسیب پذیری های منع سرویس
  - N/A مشخص کننده آسیب پذیری هایی که دسته بندی آنها در دسترس نیست.

۱-۲ آسیب پذیری بخش Framework

شدیدترین آسیب پذیری ها در این بخش منجر به افزایش امتیاز محلی بدون نیاز به امتیاز اجرایی اضافی می‌شود.

شناسه CVE	منبع	نوع	شدت	نسخه های AOSP به روز شده
CVE-2023-40106	A-278558814	EoP	High	L, 13, 14؟ ,۱۲ ,۱۱
CVE-2023-40107	A-287298721	EoP	High	L, 13, 14؟ ,۱۲
CVE-2023-40109	A-291299076	EoP	High	L, 13, 14؟ ,۱۲ ,۱۱
CVE-2023-40110	A-243463593	EoP	High	L, 13, 14؟ ,۱۲ ,۱۱
CVE-2023-40111	A-272024837	EoP	High	14
CVE-2023-40114	A-243381410	EoP	High	L, 13, 14؟ ,۱۲ ,۱۱
CVE-2023-40105	A-289549315	ID	High	L, 13, 14؟ ,۱۲ ,۱۱
CVE-2023-40124	A-272025416	ID	High	L, 13؟ ,۱۲ ,۱۱

۱-۳ آسیب پذیری بخش System

شدیدترین آسیب پذیری ها در این بخش منجر به افشای اطلاعات محلی بدون نیاز به امتیاز اجرایی اضافی می‌شود. طبق گفته گوگل آسیب پذیری CVE-2023-40113 شدیدترین آسیب پذیری این ماه است.

شناسه CVE	منبع	نوع	شدت	نسخه های AOSP به روز شده
CVE-2023-40113	A-289242655	ID	Critical	L, 13؟ ,۱۲ ,۱۱
CVE-2023-40100	A-278303745	EoP	High	L, 13, 14؟ ,۱۲ ,۱۱

CVE-2023-40115	A-285645039	EoP	High	L, 13, 14۱۲ ,۱۲ ,۱۱
CVE-2023-40104	A-284262845	ID	High	L, 13۱۲ ,۱۲ ,۱۱
CVE-2023-40112	A-168903843	ID	High	11
CVE-2023-21103	A-259064622 [2]	DoS	High	L, 13۱۲ ,۱۲ ,۱۱
CVE-2023-21111	A-256819769 [2]	DoS	High	L, 13۱۲ ,۱۲ ,۱۱

۱-۴ آسیب پذیری های سیستم بروزرسانی Google Play

آسیب پذیری های زیر در مولفه Project Mainline قرار گرفته‌اند.

شناسه CVE	Subcomponent
CVE-2023-40100	**DNS Resolver**
CVE-2023-40115	**Statsd**

۱-۵ بروزرسانی Kernel LTS

کرنل های زیر بروزرسانی شده‌اند. نسخه‌ی کرنل بروزشده به نسخه اندروید در زمان اجرای بستگی دارد .

منبع	نسخه راه اندازی اندروید	نسخه راه اندازی هسته	حداقل نسخه راه اندازی
A-273609724	11	5.4	5.4.233
A-273609966	12	5.4	5.4.233
A-273610287	12	5.10	5.10.168
A-273610950	13	5.10	5.10.168

A-273610973	13	5.15	5.15.94

۱-۶ آسیب پذیری بخش ARM

این آسیب پذیری‌ها برروی مولفه‌های ARM تاثیر می‌گذارند. شدت و جزییات را کمپانی ARM ارائه می‌دهد.

شناسه CVE	منبع	شدت	Subcomponent
CVE-2023-28469	A-274006187 *	High	Mali

۱-۷ آسیب پذیری بخش MediaTek

این آسیب پذیری‌ها روی مولفه‌های MediaTek تاثیر می‌گذارند. شدت و جزییات را کمپانی MediaTek ارائه می‌دهد.

شناسه CVE	منبع	شدت	Subcomponent
CVE-2023-32832	A-298879091 M-ALPS08235273 *	High	video
CVE-2023-32834	A-298879096 M-ALPS08161762 *	High	secmem
CVE-2023-32835	A-298881373 M-ALPS08157918 *	High	keyinstall
CVE-2023-32836	A-298879097 M-ALPS08126725 *	High	display
CVE-2023-32837	A-298879037 M-ALPS08235273 *	High	video
CVE-2023-20702	A-298879043 M-MOLY00921261 *	High	5G NRLC

۱-۸ آسیب پذیری بخشQualcomm

این آسیب پذیری ها برروی مولفه های Qualcomm تاثیر می‌گذارند. شدت و جزییات را کمپانی Qualcomm ارائه می‌دهند.

شناسه CVE	منبع	شدت	Subcomponent
CVE-2023-33031	A-290061915 QC-CR#3442627	High	Audio
CVE-2023-33055	A-295039120 QC-CR#3454515 [2]	High	Audio
CVE-2023-33059	A-295019252 QC-CR#3453288 [2] [3]	High	Audio
CVE-2023-33074	A-295039157 QC-CR#3434828	High	Audio

۱-۹ آسیب پذیری بخشQualcomm closed-source

آسیب پذیری ها برروی بخش Qualcomm closed-source تاثیر می‌گذارد و شدت و جزییات را کمپانی Qualcomm ارائه می‌دهد.

شناسه CVE	منبع	شدت	Subcomponent
CVE-2023-21671	A-280342069 *	Critical	Closed-source component
CVE-2023-22388	A-280341977 *	Critical	Closed-source component
CVE-2023-28574	A-280342089 *	Critical	Closed-source component
CVE-2023-33045	A-295019170 *	Critical	Closed-source component
CVE-2023-24852	A-280342090 *	High	Closed-source component
CVE-2023-28545	A-280341536 *	High	Closed-source component
CVE-2023-28556	A-280342072 *	High	Closed-source component

Closed-source component	High	A-295039557 *	CVE-2023-33047
Closed-source component	High	A-295038661 *	CVE-2023-33048
Closed-source component	High	A-295039159 *	CVE-2023-33056
Closed-source component	High	A-295039730 *	CVE-2023-33061

۲ مراجع

۱ https://source.android.com/docs/security/bulletin/2023-11-01