MAHARASHTRA GOVERNMENT
SPECIAL INSPECTOR GENARAL OF POLICE MAHARASHTRA
CYBER, WORLD TRADE CENTER, CUFFE PARED-400005
Email: sp.cbr-mah@gov.in

Multiple Android Vulnerabilities Advisory

The Maharashtra Computer Emergency Response Team (MHCERT) has identified multiple high-risk vulnerabilities in Android that pose a significant threat to users and organizations worldwide. This advisory provides insights into the vulnerabilities, their potential impacts, and mitigation strategies to protect against exploitation.

Key Highlights of the Advisory:

- **Targeted Versions:** Android versions 12, 12L, 13, 14, and 15 are affected.
- **Exploited CVEs:** CVE-2024-53104 (Kernel privilege escalation) has been actively exploited in the wild, increasing the risk of attacks.
- **Impact of Attacks**:
  - **Remote Code Execution:** Attackers can run arbitrary code, install malware, or take control of devices.
  - **Privilege Escalation:** Malicious actors can gain higher access and bypass security restrictions.
  - **Denial of Service:** Targeted devices may crash or become unusable.
  - **Information Disclosure:** Sensitive user data, including messages and credentials, can be stolen.
- **Recent Incidents: CVE-2024-53104** has been exploited in targeted attacks, leading to full device compromise.
- **Mitigation Strategies:** The advisory includes actionable recommendations such as:
  - **Apply Security Patches:** Install the latest Android security updates to mitigate known vulnerabilities.
  - **Enable Google Play Protect:** Use built-in security features to detect and block harmful apps.
  - **Restrict App Permissions:** Review and limit app access to sensitive data.
  - **Enhance Phishing Awareness:** Be cautious of suspicious emails, messages, and app downloads.
  - **Backup Critical Data:** Maintain offline backups to recover from data loss due to attacks.

TLP:CLEAR

MAHACYBER ADVISORY

Multiple Vulnerabilities in Android

MHCERT

ADVISORY ID: CERTMH_VA_2025_01

DATE: 10th February 2025

TABLE OF CONTENT

Summary

Severity Rating: High

Attribute	Details
Attacks	Multiple Vulnerabilities
Vendor	Android
Targeted Version	Android Versions: 12, 12L, 13, 14, and 15
Target Audience	All OEMs and users of Android
Exploited	Yes, Exploited in the wild
High-Risk CVE-ID	CVE-2024-53104 (**Critical Score: 7.8**)

Overview

Multiple vulnerabilities have been reported in Android which could be exploited by an attacker to obtain sensitive information, gain elevated privilege, execute arbitrary code or cause denial of service (DoS) condition on the targeted system.

Risk Assessment:
High risk of unauthorized access to data and system instability.

Impact Assessment:
Potential for unauthorized access to sensitive user information, privilege escalation, system compromise.

Vulnerabilities Details

Title	Reference	Severity	Impact	CVE
Android	A-354682735	High	Elevation of Privilege (EoP)	CVE-2024-49721
	A-305695605	High	Elevation of Privilege (EoP)	CVE-2024-49743
	A-359179312	High	Elevation of Privilege (EoP)	CVE-2024-49746
	A-364037868	High	Elevation of Privilege (EoP)	CVE-2025-0097
	A-367266072	High	Elevation of Privilege (EoP)	CVE-2025-0098
	A-370962373	High	Elevation of Privilege (EoP)	CVE-2025-0099
	A-286235483	High	Information Disclosure (ID)	CVE-2023-40122
	A-283264674	High	Information Disclosure (ID)	CVE-2023-40133
	A-283101289	High	Information Disclosure (ID)	CVE-2023-40134
	A-281848557	High	Information Disclosure (ID)	CVE-2023-40135
	A-281666022	High	Information Disclosure (ID)	CVE-2023-40136
	A-281665050	High	Information Disclosure (ID)	CVE-2023-40137
	A-281534749	High	Information Disclosure (ID)	CVE-2023-40138
	A-281533566	High	Information Disclosure (ID)	CVE-2023-40139
	A-292104015	High	Information Disclosure (ID)	CVE-2024-0037
	A-372670004	High	Information Disclosure (ID)	CVE-2025-0100
	A-353240784	High	Denial of Service (DoS)	CVE-2024-49741
Platform	A-352542820	High	Elevation of Privilege (EoP)	CVE-2025-0094
System	A-366401629	High	Elevation of Privilege (EoP)	CVE-2025-0091
	A-356117796	High	Elevation of Privilege (EoP)	CVE-2025-0095
	A-356630194	High	Elevation of Privilege (EoP)	CVE-2025-0096

	A-357870429	High	Information Disclosure (ID)	CVE-2024-49723
	A-368069390	High	Information Disclosure (ID)	CVE-2024-49729
Google Play system updates	Conscrypt	High	Information Disclosure (ID)	CVE-2024-49723
Kernel	A-378455392 Upstream kernel	High	Elevation of Privilege (EoP)	CVE-2024-53104
	A-377672115 Upstream kernel	High	Elevation of Privilege (EoP)	CVE-2025-0088
Arm Components	A-376311652	High	Elevation of Privilege (EoP)	CVE-2025-0015
Imagination Technologies	A-372931317, PP-160756	High	Elevation of Privilege (EoP)	CVE-2024-43705
	A-379728401, PP-160739	High	Elevation of Privilege (EoP)	CVE-2024-46973
	A-365954523, PP-160576	High	Elevation of Privilege (EoP)	CVE-2024-47892
	A-380478495, PP-171230	High	Elevation of Privilege (EoP)	CVE-2024-52935
MediaTek Components	A-381773169, M-MOLY01289384	High	Elevation of Privilege (EoP)	CVE-2025-20634
	A-381773173, M-ALPS09291402	High	Elevation of Privilege (EoP)	CVE-2024-20141
	A-381773175, M-ALPS09291406	High	Elevation of Privilege (EoP)	CVE-2024-20142
	A-381771695, M-ALPS09403752	High	Elevation of Privilege (EoP)	CVE-2025-20635
	A-381773171, M-ALPS09403554	High	Elevation of Privilege (EoP)	CVE-2025-20636
Unisoc Components	A-381429835, U-2811333	High	Elevation of Privilege (EoP)	CVE-2024-39441
Qualcomm Components	A-377311993, QC-CR#3852339	Critical	Remote Code Execution (RCE)	CVE-2024-45569
	A-377313069, QC-CR#3834424	High	Remote Code Execution (RCE)	CVE-2024-45571
	A-377312377, QC-CR#3868093 A-377312238	High	Remote Code Execution (RCE)	CVE-2024-45582

Software Affected

Android Versions: 12, 12L, 13, 14, and 15

Resolution

Apply the security updates mentioned here

Best Practices for Android Users

- **Keep your device updated:** Install the latest security patches to protect against vulnerabilities.
- **Download apps from trusted sources:** Use the Google Play Store and avoid third-party or unknown sources.
- **Enable Google Play Protect:** Enable it to detect and block potentially harmful apps.
- **Review app permissions:** Restrict unnecessary access to your data.
- **Be careful with links:** Avoid clicking on suspicious links in emails or messages.
- **Back up your data regularly:** Store backups securely in the cloud or on external storage.

References

Android Security Updates dated February 2025
https://source.android.com/docs/security/bulletin/2025-02-01