July 3, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released Android Security Bulletin. The vulnerability affects Android Open Source Project (AOSP) versions 12, 12L, 13, and 14.

Technical Details

The most severe of these issues is a critical security vulnerability in the Framework component that could lead to local escalation of privilege with no additional execution privileges needed. The severity assessment is based on the effect that exploiting the vulnerability would possibly have on an affected device, assuming the platform and service mitigations are turned off for development purposes or if successfully bypassed.

In the references below, there are details for each of the security vulnerabilities that apply to the 2024-07-01 patch. Vulnerabilities are grouped under the component they affect. Security patch levels of 2024-07-05 or later address all reported vulnerabilities.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-0153, CVE-2024-20076, CVE-2024-20077, CVE-2024-21460, CVE-2024-21461, CVE-2024-21462, CVE-2024-21465, CVE-2024-21469, CVE-2024-23368, CVE-2024-23372, CVE-2024-23373, CVE-2024-23380, CVE-2024-26923, CVE-2024-31320, CVE-2024-31331, CVE-2024-31332, CVE-2024-31334, CVE-2024-31335, CVE-2024-31339, CVE-2024-34720, CVE-2024-34721, CVE-2024-34722, CVE-2024-34723, CVE-2024-34724, CVE-2024-34725, CVE-2024-34726, CVE-2024-4610
- Android Security Bulletin—July 2024
- VRM Vulnerability Reports