UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 0339

## GOOGLE ANDROID OS VULNERABILITIES ENABLE RCE

**DATE ISSUED:** 9th August 2023

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | HIGH |
| EASE OF EXPLOIT | HARD | MEDIUM | EASY |

## OVERVIEW

A series of vulnerabilities have been detected within the Google Android OS, with the most significant among them being capable of enabling remote code execution.

## BREAKDOWN

Android, an operating system created by Google, is designed for various mobile devices, encompassing smartphones, tablets, and smartwatches, among others. Numerous flaws were found in Google's Android OS, with the most critical permitting remote code execution. Depending on the level of access granted to the compromised system, an attacker could potentially install software, manipulate or remove data, or establish new accounts with complete privileges. The most severe vulnerabilities in Kernel tracked as CVE-2023-21264 and CVE-2020-29374 could lead to local escalation of privilege with System execution privileges. The system affected is Android OS patch levels prior to 2023-08-05.

## REMEDIATION STEPS

- Apply security updates provided by Google after appropriate testing.
- Conduct automated vulnerability assessments on enterprise assets accessible externally. Perform these scans on a monthly or more regular schedule.
- Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise.
- Employ robust monitoring and intrusion detection systems to promptly identify and respond to any suspicious or unauthorised activities.

## REFERENCES & RESOURCES

| | |
|---|---|
| AOSP | https://source.android.com/docs/security/bulletin/2023-08-01 |
| MS ISAC Advisory | https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-fovr-remote-code-execution_2023-089 |