

ADVISORY !

TLP : CLEAR

DATE : 9th Nov 2023

REF NO : CERT/ NCSOC /0203

Multiple Vulnerabilities in Google Android OS

Severity Level: **Medium**

Components Affected

- Android security patch level prior to 2023-11-05

Overview

Multiple vulnerabilities were identified in Google Android OS. A remote attacker could exploit some of these vulnerabilities to trigger denial of service condition, privilege escalation and sensitive information disclosure on the targeted system.

Description

Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for privilege escalation. Depending on the privileges associated with the exploited component, an attacker could then install programs; view, change, or delete data; or create new accounts with full rights.

Impact

- Privilege Escalation
- Denial of Service
- Information Disclosure

Solution/ Workarounds

Before installation of the software, please visit the software vendor web-site for more details.

- Apply fixes issued by the vendor:
<https://source.android.com/docs/security/bulletin/2023-11-01>

Reference

- https://www.hkcert.org/security-bulletin/android-multiple-vulnerabilities_20231108
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-privilege-escalation_2023-130

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.