CVE-2026-0073

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0073
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 18:16:26 UTC
Updated	2026-05-05 19:54:49 UTC
Description	In adbd_tls_verify_cert of auth.cpp, there is a possible bypass of wireless ADB mutual authentication due to a logic error in

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from ADP

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000110000 probability, percentile 0.014860000 (date 2026-05-05)

Problem Types: CWE-303 | Remote code execution | CWE-303 CWE-303 Incorrect Implementation of Authentication Algorithm

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	14.0	All	All	All
Operating System	Google	Android	15.0	All	All	All
Operating System	Google	Android	16.0	-	All	All
Operating System	Google	Android	16.0	qpr2_beta_1	All	All
Operating System	Google	Android	16.0	qpr2_beta_2	All	All
Operating System	Google	Android	16.0	qpr2_beta_3	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google	Android	affected 16-qpr2	Not specified
CNA	Google	Android	affected 16	Not specified
CNA	Google	Android	affected 15	Not specified
CNA	Google	Android	affected 14	Not specified

References

Reference	Source	Link	Tags
source.android.com/docs/security/bulletin/2026/2026-05-01	security@android.com	source.android.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Ovi (@0x0v1 + Barghest.asia) (en)

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report