apko doesn't verify downloaded apk packages against APKINDEX checksum (package substitution possible)

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

Summary

CVE	CVE-2026-42575
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-09 20:16:29 UTC
Updated	2026-05-09 20:16:29 UTC
Description	apko allows users to build and publish OCI container images built from apk packages. Prior to version 1.2.7, apko verifies th

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

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

Problem Types: CWE-345 | CWE-494 | CWE-345 CWE-345: Insufficient Verification of Data Authenticity | CWE-494 CWE-494: Download of Code Without Integrity Check

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Chainguard-dev	Apko	affected < 1.2.7	Not specified

References

Reference	Source	Link	Tag
github.com/chainguard-dev/apko/releases/tag/v1.2.7	security-advisories@github.com	github.com	
github.com/chainguard-dev/apko/security/advisories/GHSA-hcwr-pq9g-rq3m	security-advisories@github.com	github.com	
github.com/chainguard-dev/apko/commit/a118c3d604107532b5525bd4bee2fb369a...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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