



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-42575
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-09 20:16:29 UTC
<b>Updated</b>	2026-05-09 20:16:29 UTC
<b>Description</b>	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

High

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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)