Cosign's verify-blob-attestation reports false positive when payload parsing fails

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

Summary

CVE	CVE-2026-39395
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 20:16:33 UTC
Updated	2026-04-08 21:27:00 UTC
Description	Cosign provides code signing and transparency for containers and binaries. Prior to 3.0.6 and 2.6.3, cosign verify-blob-attes

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from security-advisories@github.com

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

EPSS: 0.000290000 probability, percentile 0.082460000 (date 2026-04-09)

Problem Types: CWE-754 | CWE-754 CWE-754: Improper Check for Unusual or Exceptional Conditions

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sigstore	Cosign	affected >= 3.0.0, < 3.0.6	Not specified
CNA	Sigstore	Cosign	affected < 2.6.3	Not specified

References

Reference	Source	Link	Tags
github.com/sigstore/cosign/security/advisories/GHSA-w6c6-c85g-mmv6	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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