



# Step CA affected by an index out of bounds panic in TPM attestation EKU validation

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

## Summary

<b>CVE</b>	CVE-2026-40097
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-10 17:17:12 UTC
<b>Updated</b>	2026-04-10 17:17:12 UTC
<b>Description</b>	Step CA is an online certificate authority for secure, automated certificate management for DevOps. From 0.24.0 to before (

## Risk And Classification

**Primary CVSS:** v3.1 3.7 LOW from security-advisories@github.com

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

**Problem Types:** CWE-129 | CWE-129 CWE-129: Improper Validation of Array Index

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	3.7	LOW	<b>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L</b>
3.1	CNA	DECLARED	3.7	LOW	<b>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**None**

Integrity

**None**

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Smallstep	Certificates	affected >= 0.24.0, < 0.30.0-rc3	Not specified

### References

Reference	Source	Link	Tags
github.com/smallstep/certificates/commit/ffd31ac0a87e03b0224cb8363094bfe...	security-advisories@github.com	github.com	
github.com/smallstep/certificates/pull/2569	security-advisories@github.com	github.com	
github.com/smallstep/certificates/releases/tag/v0.30.0	security-advisories@github.com	github.com	
github.com/smallstep/certificates/security/advisories/GHSA-9qq8-cgcv-qmc9	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)