



# jq: Missing runtime type checks for `_strindices` lead to crash and limited memory disclosure

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

## Summary

<b>CVE</b>	CVE-2026-39956
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 23:16:27 UTC
<b>Updated</b>	2026-04-13 23:16:27 UTC
<b>Description</b>	jq is a command-line JSON processor. In commits after 69785bf77f86e2ea1b4a20ca86775916889e91c9, the <code>_strindices</code> b

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from security-advisories@github.com

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

**Problem Types:** CWE-125 | CWE-476 | CWE-843 | CWE-125 CWE-125: Out-of-bounds Read | CWE-476 CWE-476: NULL Pointer Dereference | CWE-843 CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
--------	--------	---------	---------

CNA	Jqlang	Jq	affected >= 69785bf77f86e2ea1b4a20ca86775916889e91c9, < fdf8ef0f0810e3d365cdd5160de43db46f57ed03
-----	--------	----	--

### References

Reference	Source	Link	Tags
github.com/jqlang/jq/security/advisories/GHSA-6gc3-3g9p-xx28	security-advisories@github.com	github.com	
github.com/jqlang/jq/commit/fdf8ef0f0810e3d365cdd5160de43db46f57ed03	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)