



# CVE-2026-31252

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31252
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-11 17:16:20 UTC
<b>Updated</b>	2026-05-12 20:16:33 UTC
<b>Description</b>	CosyVoice thru commit 6e01309e01bc93bbeb83bdd996b1182a81aaf11e (2025-30-21) contains an insecure deserializator

## Risk And Classification

**Primary CVSS:** v3.1 5.7 MEDIUM from ADP

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

**EPSS:** 0.000190000 probability, percentile 0.054610000 (date 2026-05-12)

**Problem Types:** CWE-94 | CWE-915 | n/a | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection') | CWE-915 CWE-915 Improperly Controlled Modification of Dynamically-Determined Object Attributes

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source	Link	Tags
github.com/FunAudioLLM/CosyVoice	cve@mitre.org	github.com	
www.notion.so/CVE-2026-31252-35d1e139318881ef8acfd877a432569	cve@mitre.org	www.notion.so	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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)