



CVE-2022-29266

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-29266
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-20 08:15:00 UTC
Updated	2022-04-29 23:38:00 UTC
Description	In APache APISIX before 3.13.1, the jwt-auth plugin has a security issue that leaks the user's secret key because the error

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Apisix	All	All	All	All

References

Reference	Source	Link	Tags
lists.apache.org/thread/6qpfyxogbvn18g9xr8g218jjfbfsbhr	MISC	lists.apache.org	
oss-security - CVE-2022-29266: Apache APISIX: apisix/jwt-auth may leak secrets in error response	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

LEGACY: Discovered and reported by a team from Kingdee Software (China) Ltd. consisting of Zhongyuan Tang, Hongfeng Xie, and Bing Chen.

Legacy QID Mappings

[730614 Apache Apisix Sensitive Information Disclosure Vulnerability](#)

© [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](#)