



CVE-2022-30973

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

Summary

CVE	CVE-2022-30973
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-31 14:15:00 UTC
Updated	2022-10-27 16:41:00 UTC
Description	We failed to apply the fix for CVE-2022-30126 to the 1.x branch in the 1.28.2 release. In Apache Tika, a regular expression

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
oss-security - CVE-2022-33879: Apache Tika: Incomplete fix and new regex DoS in StandardsExtractingContentHandler	MLIST	www.oss-security.com
oss-security - CVE-2022-30973: Apache Tika: Missing fix for CVE-2022-30126 in 1.28.2	MLIST	www.oss-security.com
N/A	CONFIRM	lists.apache.org
CVE-2022-30973 Apache Tika Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was reported by Cathy Hu, SUSE Software Solutions Germany GmbH.

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](#)