



CVE-2022-4065

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

Summary

CVE	CVE-2022-4065
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-19 19:15:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	A vulnerability was found in cbeust testng 7.5.0/7.6.0/7.6.1/7.7.0. It has been declared as critical. Affected by this vulnerabil

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Testng Project	Testng	-	All	All	All

References

Reference	Source	Link
Login required	MISC	vuldb.com
[SECURITY] Fix Zip Slip Vulnerability by JLLeitschuh · Pull Request #2806 · cbeust/testng · GitHub	N/A	github.com
Release TestNG v7.7.1 · cbeust/testng · GitHub	MISC	github.com
CVE-2022-4065 cbeust testng XML File Parser JarFileUtils.java testngXmlExistsInJar path traversal (ID 2806)	N/A	vuldb.com
Merge pull request #2806 from BulkSecurityGeneratorProjectV2/fix/JLL/... · cbeust/testng@9150736 · GitHub	N/A	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[753876](#) SUSE Enterprise Linux Security Update for testng (SUSE-SU-2023:1690-1)

© [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](#)