



CVE-2021-30638

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

Summary

CVE	CVE-2021-30638
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-27 19:15:00 UTC
Updated	2022-10-27 12:42:00 UTC
Description	Information Exposure vulnerability in context asset handling of Apache Tapestry allows an attacker to download files inside

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
oss-security - CVE-2021-30638: An Information Disclosure due to insufficient input validation exists in Apache Tapestry 5.4.0 and later	MLIS
CVE-2021-30638 Apache Tapestry Vulnerability in NetApp Products NetApp Product Security	CON
ZDI-21-491 Zero Day Initiative	MISC
Pony Mail!	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability was discovered by Kc Udonsi of Trend Micro

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](#)