



CVE-2020-17531

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

Summary

CVE	CVE-2020-17531
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-08 13:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A Java Serialization vulnerability was found in Apache Tapestry 4. Apache Tapestry 4 will attempt to deserialize the "sp" pa

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
oss-security - CVE-2022-46366: Apache Tapestry prior to version 4 (EOL) allows RCE though deserialization of untrusted input	MLIST
Pony Mail!	MLIST
CVE-2020-17531 Apache Tapestry Vulnerability in NetApp Products NetApp Product Security	CONFIRM
Pony Mail!	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Tapestry would like to thank Adrian Bravo (@adrianbravon) for reporting this issue.

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](#)