



CVE-2021-27850

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

Summary

CVE	CVE-2021-27850
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-15 08:15:00 UTC
Updated	2021-06-02 15:15:00 UTC
Description	A critical unauthenticated remote code execution vulnerability was found all recent versions of Apache Tapestry. The affect

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

References

Reference	Source	Link	Tags
CVE-2021-27850 Apache Tapestry Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Pony Mail!	MISC	lists.apache.org	
oss-security - CVE-2021-27850: Apache Tapestry: Bypass of the fix for CVE-2019-0195	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Tapestry would like to thank Johannes Moritz for finding and notifying this vulnerability

Legacy QID Mappings

730165 Apache Tapestry Remote Code Execution Vulnerability Detected

© [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](#)