



CVE-2018-17187

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

Summary

CVE	CVE-2018-17187
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-13 15:29:00 UTC
Updated	2019-01-31 19:10:00 UTC
Description	The Apache Qpid Proton-J transport includes an optional wrapper layer to perform TLS, enabled by use of the 'transport.ss

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Qpid Proton-j	All	All	All	All

References

Reference	Source	Li
Apache Qpid Proton-J CVE-2018-17187 Certificate Validation Security Bypass Vulnerability	BID	wv
[PROTON-1962] [CVE-2018-17187] transport TLS wrapper hostname verification mode not implemented - ASF JIRA	MISC	isc
CVE-2018-17187: transport TLS wrapper hostname verification mode not implemented - Apache Qpid™	MISC	qp
[SECURITY] [CVE-2018-17187] Apache Qpid Proton-J transport TLS wrapper hostname verification mode not implemented	MISC	m
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980776 Java (maven) Security Update for org.apache.qpid:proton-j (GHSA-xvch-r4wf-h8w9)

© [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](#)