



CVE-2018-8020

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

Summary

CVE	CVE-2018-8020
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-31 13:29:00 UTC
Updated	2023-11-07 03:01:00 UTC
Description	Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 has a flaw that does not properly check OCSP pre-produced res

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat Native	All	All	All	All
Application	Apache	Tomcat Native	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

References

Reference

- Apache Tomcat Native Connector CVE-2018-8020 Remote Security Vulnerability
- [SECURITY] CVE-2018-8020 Apache Tomcat Native Connector - Mishandled OCSP responses can allow clients to authenticate with revoked
- Apache Mail Archives
- Pony Mail!
- Pony Mail!
- Pony Mail!
- [SECURITY] [DLA 1475-1] tomcat-native security update
- Pony Mail!
- Pony Mail!
- Red Hat Customer Portal

Apache Mail Archives

[SECURITY] CVE-2018-8020 Apache Tomcat Native Connector - Mishandled OCSP responses can allow clients to authenticate with revoked

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Apache Tomcat Native OCSP Response Handling Flaws Let Remote Users Bypass Authentication on the Target System - SecurityTracker

Apache Mail Archives

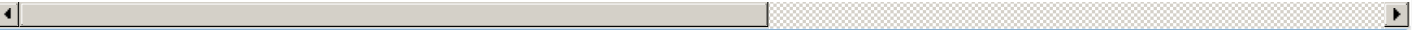
Pony Mail!

Apache Mail Archives

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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](#)