CVE-2018-8034

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-8034
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-01 18:29:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions A

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All
Application	Apache	Tomcat	8.0.0	rc4	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.0	rc6	All	All
Application	Apache	Tomcat	8.0.0	rc7	All	All
Application	Apache	Tomcat	8.0.0	rc8	All	All
Application	Apache	Tomcat	8.0.0	rc9	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All

Application	Apache	Tomcat	9.0.0	m16	All	All
Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m2	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All
Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m22	All	All
Application	Apache	Tomcat	9.0.0	m23	All	All
Application	Apache	Tomcat	9.0.0	m24	All	All
Application	Apache	Tomcat	9.0.0	m25	All	All
Application	Apache	Tomcat	9.0.0	m26	All	All
Application	Apache	Tomcat	9.0.0	m27	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All
Application	Apache	Tomcat	9.0.0	m4	All	All
Application	Apache	Tomcat	9.0.0	m5	All	All
Application	Apache	Tomcat	9.0.0	m6	All	All
Application	Apache	Tomcat	9.0.0	m7	All	All
Application	Apache	Tomcat	9.0.0	m8	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All
Application	Apache	Tomcat	9.0.0	milestone1	All	All
Application	Apache	Tomcat	9.0.0	milestone10	All	All
Application	Apache	Tomcat	9.0.0	milestone11	All	All
Application	Apache	Tomcat	9.0.0	milestone12	All	All
Application	Apache	Tomcat	9.0.0	milestone13	All	All
Application	Apache	Tomcat	9.0.0	milestone14	All	All
Application	Apache	Tomcat	9.0.0	milestone15	All	All
Application	Apache	Tomcat	9.0.0	milestone16	All	All
Application	Apache	Tomcat	9.0.0	milestone17	All	All
Application	Apache	Tomcat	9.0.0	milestone18	All	All
Application	Apache	Tomcat	9.0.0	milestone19	All	All
Application	Apache	Tomcat	9.0.0	milestone2	All	All
Application	Apache	Tomcat	9.0.0	milestone20	All	All
Application	Apache	Tomcat	9.0.0	milestone21	All	All
Application	Apache	Tomcat	9.0.0	milestone22	All	All

Application	Apache	Tomcat	9.0.0	milestone23	All	All
Application	Apache	Tomcat	9.0.0	milestone24	All	All
Application	Apache	Tomcat	9.0.0	milestone25	All	All
Application	Apache	Tomcat	9.0.0	milestone26	All	All
Application	Apache	Tomcat	9.0.0	milestone27	All	All
Application	Apache	Tomcat	9.0.0	milestone3	All	All
Application	Apache	Tomcat	9.0.0	milestone4	All	All
Application	Apache	Tomcat	9.0.0	milestone5	All	All
Application	Apache	Tomcat	9.0.0	milestone6	All	All
Application	Apache	Tomcat	9.0.0	milestone7	All	All
Application	Apache	Tomcat	9.0.0	milestone8	All	All
Application	Apache	Tomcat	9.0.0	milestone9	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All
Application	Apache	Tomcat	8.0.0	rc4	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.0	rc6	All	All
Application	Apache	Tomcat	8.0.0	rc7	All	All
Application	Apache	Tomcat	8.0.0	rc8	All	All
Application	Apache	Tomcat	8.0.0	rc9	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All
Application	Apache	Tomcat	9.0.0	m16	All	All
Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m2	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All

Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m22	All	All
Application	Apache	Tomcat	9.0.0	m23	All	All
Application	Apache	Tomcat	9.0.0	m24	All	All
Application	Apache	Tomcat	9.0.0	m25	All	All
Application	Apache	Tomcat	9.0.0	m26	All	All
Application	Apache	Tomcat	9.0.0	m27	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All
Application	Apache	Tomcat	9.0.0	m4	All	All
Application	Apache	Tomcat	9.0.0	m5	All	All
Application	Apache	Tomcat	9.0.0	m6	All	All
Application	Apache	Tomcat	9.0.0	m7	All	All
Application	Apache	Tomcat	9.0.0	m8	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Oracle	Retail Order Broker	15.0	All	All	All
Application	Oracle	Retail Order Broker	5.1	All	All	All
Application	Oracle	Retail Order Broker	5.2	All	All	All
Application	Oracle	Retail Order Broker	15.0	All	All	All
Application	Oracle	Retail Order Broker	5.1	All	All	All
Application	Oracle	Retail Order Broker	5.2	All	All	All

References

Reference
Pony Mail!

USN-3723-1: Tomcat vulnerabilities | Ubuntu security notices

Pony Mail!

Red Hat Customer Portal

[SECURITY] [DLA 1453-1] tomcat7 security update

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] [DLA 1491-1] tomcat8 security update

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

[SECURITY] CVE-2018-8034 Apache Tomcat - Security Constraint Bypass

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

July 2018 Apache Tomcat Vulnerabilities in NetApp Products | NetApp Product Security

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] CVE-2018-8034 Apache Tomcat - Security Constraint Bypass

Pony Mail!

Pony Mail!

Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update - July 2019
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Apache Tomcat CVE-2018-8034 Security Bypass Vulnerability
Apache Tomcat Missing Check in WebSocket Client Lets Remote Users Bypass Hostname Verification on the Target System - SecurityTracke
CPU Oct 2018
Pony Mail!
Oracle Critical Patch Update - October 2019
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - April 2020
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Debian -- Security Information -- DSA-4281-1 tomcat8
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - April 2019
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

940573 AlmaLinux Security Update for pki-deps:10.6 (ALSA-2019:1529)

960759 Rocky Linux Security Update for pki-deps:10.6 (RLSA-2019:1529)

981328 Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-46j3-r4pj-4835)

CVE.report and Source URL Uptime Status status.cve.report