



CVE-2018-8014

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-8014
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-16 16:29:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52,

Risk And Classification

Problem Types: CWE-1188

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	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	milestone1	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	9.0.0	m1	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Snapcenter Server	-	All	All	All
Application	Netapp	Snapcenter Server	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All

References

Reference
Pony Mail!
Pony Mail!
Bugtraq: [SECURITY] [DSA 4596-1] tomcat8 security update
Pony Mail!
Apache Tomcat CVE-2018-8014 Security Bypass Vulnerability
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
[SECURITY] [DLA 1400-1] tomcat7 security update
Red Hat Customer Portal

Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Debian -- Security Information -- DSA-4596-1 tomcat8
Pony Mail!
MySQL Multiple Flaws Let Remote Users Gain Elevated Privileges, Remote Authenticated Users Access and Modify Data, and Remote and L
Pony Mail!
Apache Tomcat Default CORS Filter Settings Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Apache Mail Archives
USN-3665-1: Tomcat vulnerabilities Ubuntu security notices
Red Hat Customer Portal
Apache Mail Archives
Pony Mail!
October 2018 MySQL Vulnerabilities in NetApp Products NetApp Product Security
Pony Mail!
Pony Mail!
[SECURITY] [DLA 1883-1] tomcat8 security update
Apache Tomcat® - Apache Tomcat 7 vulnerabilities
Apache Tomcat® - Apache Tomcat 8 vulnerabilities
CPU Oct 2018
Pony Mail!
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - April 2020
Pony Mail!

