CVE-2020-1938

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1938
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-24 22:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat.

Risk And Classification

EPSS: 0.944690000 probability, percentile 0.999970000 (date 2026-04-01)

CISA KEV: Listed on 2022-03-03; due 2022-03-17; ransomware use Unknown

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Tomcat
Name	Apache Tomcat Improper Privilege Management Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-1938

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Geode	1.12.0	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Blackberry	Good Control	All	All	All	All
Application	Blackberry	Workspaces Server	7.0.1	All	All	All
Application	Blackberry	Workspaces Server	7.1.2	All	All	All
Application	Blackberry	Workspaces Server	8.1.0	All	All	All

Application	Blackberry	Workspaces Server	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	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	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Agile Engineering Data Management	6.2.1.0	All	All	All
Application	Oracle	Agile Plm	9.3.3	All	All	All
Application	Oracle	Agile Plm	9.3.5	All	All	All
Application	Oracle	Agile Plm	9.3.6	All	All	All
Application	Oracle	Communications Element Manager	8.1.1	All	All	All
Application	Oracle	Communications Element Manager	8.2.0	All	All	All
Application	Oracle	Communications Element Manager	8.2.1	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.4.0	All	All	All
Application	Oracle	Health Sciences Empirica Inspections	1.0.1.2	All	All	All
Application	Oracle	Health Sciences Empirica Signal	7.3.3	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Siebel Ui Framework	All	All	All	All
Application	Oracle	Transportation Management	6.3.7	All	All	All
Application	Oracle	Workload Manager	12.2.0.1	All	All	All
Application	Oracle	Workload Manager	18c	All	All	All
Application	Oracle	Workload Manager	19c	All	All	All

References

Reference	
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] Fedora 30 Update: tomcat-9.0.31-2.fc30 - package-announce - Fedora Mailing-Lists

Pony Mail!

Pony Mail!

Pony Mail!

BSRT-2020-001 Local File Inclusion Vulnerability in Apache Tomcat Impacts BlackBerry Workspaces Server and BlackBerry Good Control

CVE-2020-1938 Apache Tomcat Vulnerability in NetApp Products | NetApp Product Security

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] Fedora 31 Update: tomcat-9.0.31-2.fc31 - package-announce - Fedora Mailing-Lists

Pony Mail!

Oracle Critical Patch Update Advisory - July 2020

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] Fedora 32 Update: tomcat-9.0.31-2.fc32 - package-announce - Fedora Mailing-Lists

Pony Mail!

[SECURITY] [DLA 2133-1] tomcat7 security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - October 2020

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[security-announce] openSUSE-SU-2020:0345-1: important: Security update
Debian -- Security Information -- DSA-4673-1 tomcat8
[SECURITY] Fedora 32 Update: tomcat-9.0.31-2.fc32 - package-announce - Fedora Mailing-Lists
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Apache Tomcat: Multiple vulnerabilities (GLSA 202003-43) — Gentoo security
[SECURITY] [DLA 2209-1] tomcat8 security update
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Debian -- Security Information -- DSA-4680-1 tomcat9
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
[security-announce] openSUSE-SU-2020:0597-1: important: Security update
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!

Pony Mail!	I
Pony Mail!	
[SECURITY] Fedora 31 Update: tomcat-9.0.31-2.fc31 - package-announce - Fedora Mailing-Lists	I
[SECURITY] Fedora 30 Update: tomcat-9.0.31-2.fc30 - package-announce - Fedora Mailing-Lists	
Pony Mail!	I
Pony Mail!	
Pony Mail!	I
Pony Mail!	
Pony Mail!	I
Pony Mail!	I
Pony Mail!	
Oracle Critical Patch Update Advisory - January 2021	I
Pony Mail!	I
Pony Mail!	
CVE Program record	(
NVD vulnerability detail	I
CISA Known Exploited Vulnerabilities catalog	(

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

356190 Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-012

377084 Alibaba Cloud Linux Security Update for tomcat (ALINUX2-SA-2020:0032)

730112 Atlassian Jira Component Apache Tomcat Hypertext Transfer Protocol (HTTP) Request Smuggling Vulnerability (JRASERVER-70993)

730434 Update TITLE manually (JRASERVER-70487)

730441 Atlassian Jira Local Privilege Escalation Vulnerability (JRASERVER-70487)

730449 (JRASERVER-70487)

730510 Atlassian Jira Remote Code Execution (RCE) Vulnerability (JRASERVER-73223)

981939 Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-c9hw-wf7x-jp9j)

© 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 registred 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.

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