



# CVE-2014-0227

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2014-0227                                                                                                               |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | redhat                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2015-02-16 00:59:00 UTC                                                                                                     |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                     |
| Description     | java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8. |

## Risk And Classification

**Primary CVSS:** v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:P

**Problem Types:** CWE-19 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Apache | Tomcat  | 6.0.0   | All    | All     | All      |

|             |                        |                        |        |       |     |     |
|-------------|------------------------|------------------------|--------|-------|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.0  | alpha | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.1  | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.1  | alpha | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.10 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.11 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.12 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.13 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.14 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.15 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.16 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.17 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.18 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.19 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.2  | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.2  | alpha | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.2  | beta  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.20 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.24 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.26 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.27 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.28 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.29 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.3  | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.30 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.31 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.32 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.33 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.35 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.36 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.37 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.39 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.4  | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.4  | alpha | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.41 | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.5  | All   | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.6  | All   | All | All |

|             |        |        |        |       |     |     |
|-------------|--------|--------|--------|-------|-----|-----|
| Application | Apache | Tomcat | 6.0.6  | alpha | All | All |
| Application | Apache | Tomcat | 6.0.7  | All   | All | All |
| Application | Apache | Tomcat | 6.0.7  | alpha | All | All |
| Application | Apache | Tomcat | 6.0.7  | beta  | All | All |
| Application | Apache | Tomcat | 6.0.8  | All   | All | All |
| Application | Apache | Tomcat | 6.0.8  | alpha | All | All |
| Application | Apache | Tomcat | 6.0.9  | All   | All | All |
| Application | Apache | Tomcat | 6.0.9  | beta  | All | All |
| Application | Apache | Tomcat | 7.0.0  | All   | All | All |
| Application | Apache | Tomcat | 7.0.0  | beta  | All | All |
| Application | Apache | Tomcat | 7.0.1  | All   | All | All |
| Application | Apache | Tomcat | 7.0.10 | All   | All | All |
| Application | Apache | Tomcat | 7.0.11 | All   | All | All |
| Application | Apache | Tomcat | 7.0.12 | All   | All | All |
| Application | Apache | Tomcat | 7.0.13 | All   | All | All |
| Application | Apache | Tomcat | 7.0.14 | All   | All | All |
| Application | Apache | Tomcat | 7.0.15 | All   | All | All |
| Application | Apache | Tomcat | 7.0.16 | All   | All | All |
| Application | Apache | Tomcat | 7.0.17 | All   | All | All |
| Application | Apache | Tomcat | 7.0.18 | All   | All | All |
| Application | Apache | Tomcat | 7.0.19 | All   | All | All |
| Application | Apache | Tomcat | 7.0.2  | All   | All | All |
| Application | Apache | Tomcat | 7.0.2  | beta  | All | All |
| Application | Apache | Tomcat | 7.0.20 | All   | All | All |
| Application | Apache | Tomcat | 7.0.21 | All   | All | All |
| Application | Apache | Tomcat | 7.0.22 | All   | All | All |
| Application | Apache | Tomcat | 7.0.23 | All   | All | All |
| Application | Apache | Tomcat | 7.0.24 | All   | All | All |
| Application | Apache | Tomcat | 7.0.25 | All   | All | All |
| Application | Apache | Tomcat | 7.0.26 | All   | All | All |
| Application | Apache | Tomcat | 7.0.27 | All   | All | All |
| Application | Apache | Tomcat | 7.0.28 | All   | All | All |
| Application | Apache | Tomcat | 7.0.29 | All   | All | All |
| Application | Apache | Tomcat | 7.0.3  | All   | All | All |
| Application | Apache | Tomcat | 7.0.30 | All   | All | All |

|             |                        |                        |        |      |     |     |
|-------------|------------------------|------------------------|--------|------|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.31 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.32 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.33 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.34 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.35 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.36 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.37 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.38 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.39 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.4  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.4  | beta | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.40 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.41 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.42 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.43 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.44 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.45 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.46 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.47 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.48 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.49 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.5  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.50 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.52 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.53 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.54 | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.6  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.7  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.8  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 7.0.9  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.0  | rc1  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.0  | rc10 | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.0  | rc2  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.0  | rc5  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.1  | All  | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 8.0.2  | All  | All | All |

|                                                                                                                   |        |         |              |                  |     |     |
|-------------------------------------------------------------------------------------------------------------------|--------|---------|--------------|------------------|-----|-----|
| Application                                                                                                       | Apache | Tomcat  | 8.0.3        | All              | All | All |
| Application                                                                                                       | Apache | Tomcat  | 8.0.5        | All              | All | All |
| Application                                                                                                       | Apache | Tomcat  | 8.0.8        | All              | All | All |
|                                                                                                                   |        |         |              |                  |     |     |
| Vendor Declared Affected Products                                                                                 |        |         |              |                  |     |     |
| Source                                                                                                            | Vendor | Product | Version      | Platforms        |     |     |
| CNA                                                                                                               | Na     | N/a     | affected n/a | Not specified    |     |     |
|                                                                                                                   |        |         |              |                  |     |     |
| References                                                                                                        |        |         |              |                  |     |     |
| Reference                                                                                                         |        |         |              | Source           |     |     |
| USN-2654-1: Tomcat vulnerabilities   Ubuntu                                                                       |        |         |              | af854a3a-2127-.. |     |     |
| Apache Tomcat 'ChunkedInputFilter.java' Processing Flaw Lets Remote Users Smuggle HTTP Requests - SecurityTracker |        |         |              | af854a3a-2127-.. |     |     |
| Oracle Solaris Third Party Bulletin - April 2015                                                                  |        |         |              | af854a3a-2127-.. |     |     |
| '[security bulletin] HPSBUX03337 SSRT102066 rev.1 - HP-UX Apache Web Server Suite running Apache Web ' - MARC     |        |         |              | af854a3a-2127-.. |     |     |
| Support / Security / Advisories / / MDVSA-2015:053   Mandriva                                                     |        |         |              | af854a3a-2127-.. |     |     |
| Oracle Critical Patch Update - October 2016                                                                       |        |         |              | af854a3a-2127-.. |     |     |
| [SECURITY] Fedora 21 Update: tomcat-7.0.59-1.fc21                                                                 |        |         |              | af854a3a-2127-.. |     |     |
| Debian -- Security Information -- DSA-3447-1 tomcat7                                                              |        |         |              | af854a3a-2127-.. |     |     |
| Oracle Critical Patch Update - July 2015                                                                          |        |         |              | af854a3a-2127-.. |     |     |
| Apache Tomcat® - Apache Tomcat 8 vulnerabilities                                                                  |        |         |              | af854a3a-2127-.. |     |     |
| Apache Tomcat® - Apache Tomcat 7 vulnerabilities                                                                  |        |         |              | af854a3a-2127-.. |     |     |
| Red Hat Customer Portal                                                                                           |        |         |              | af854a3a-2127-.. |     |     |
| Support / Security / Advisories / / MDVSA-2015:052   Mandriva                                                     |        |         |              | af854a3a-2127-.. |     |     |
| Pony Mail!                                                                                                        |        |         |              | af854a3a-2127-.. |     |     |
| Red Hat Customer Portal                                                                                           |        |         |              | af854a3a-2127-.. |     |     |
| Pony Mail!                                                                                                        |        |         |              | af854a3a-2127-.. |     |     |
| Pony Mail!                                                                                                        |        |         |              | af854a3a-2127-.. |     |     |
| Apache Tomcat CVE-2014-0227 Chunk Request Remote Denial Of Service Vulnerability                                  |        |         |              | af854a3a-2127-.. |     |     |
| Support / Security / Advisories / / MDVSA-2015:084   Mandriva                                                     |        |         |              | af854a3a-2127-.. |     |     |
| Bug 1109196 – CVE-2014-0227 Tomcat/JBossWeb: request smuggling and limited DoS in ChunkedInputFilter              |        |         |              | af854a3a-2127-.. |     |     |
| Pony Mail!                                                                                                        |        |         |              | af854a3a-2127-.. |     |     |
| Red Hat Customer Portal                                                                                           |        |         |              | af854a3a-2127-.. |     |     |
| '[security bulletin] HPSBUX03341 SSRT102068 rev.1 - HP-UX Apache Tomcat v7.x, Remote Denial of Servic' - MARC     |        |         |              | af854a3a-2127-.. |     |     |
| FishEye: changeset 2455                                                                                           |        |         |              | af854a3a-2127-.. |     |     |
| USN-2655-1: Tomcat vulnerabilities   Ubuntu                                                                       |        |         |              | af854a3a-2127-.. |     |     |
| Pony Mail!                                                                                                        |        |         |              | af854a3a-2127-.. |     |     |
| Apache Tomcat® - Apache Tomcat 6 vulnerabilities                                                                  |        |         |              | af854a3a-2127-.. |     |     |

|                                                                              |                    |
|------------------------------------------------------------------------------|--------------------|
| Apache Tomcat® - Apache Tomcat 6 vulnerabilities                             | af854a3a-2127-4... |
| Debian -- Security Information -- DSA-3530-1 tomcat6                         | af854a3a-2127-4... |
| Red Hat Customer Portal                                                      | af854a3a-2127-4... |
| Pony Mail!                                                                   | af854a3a-2127-4... |
| NEOHAPSIS - Peace of Mind Through Integrity and Insight                      | af854a3a-2127-4... |
| Red Hat Customer Portal                                                      | af854a3a-2127-4... |
| Mageia Advisory: MGASA-2015-0081 - Updated tomcat packages fix CVE-2014-0227 | af854a3a-2127-4... |
| Pony Mail!                                                                   | af854a3a-2127-4... |
| [Apache-SVN] Revision 1600984                                                | af854a3a-2127-4... |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| Pony Mail!                                                                   | MITRE              |
| CVE Program record                                                           | CVE.ORG            |
| NVD vulnerability detail                                                     | NVD                |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.