



# CVE-2007-1355

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

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2007-1355                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | redhat                                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2007-05-21 20:30:00 UTC                                                                                                       |
| Updated         | 2026-04-23 00:35:47 UTC                                                                                                       |
| Description     | Multiple cross-site scripting (XSS) vulnerabilities in the appdev/sample/web/hello.jsp example application in Tomcat 4.0.0 th |

## Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Apache | Tomcat  | 4.0.0   | All    | All     | All      |

|             |                        |                        |        |     |     |     |
|-------------|------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.0.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.10 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.15 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.24 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.28 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.31 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.10 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.11 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.12 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.13 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.14 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.15 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.16 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.17 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.18 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.19 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.21 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.22 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.23 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.24 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.25 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.26 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.27 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.28 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.29 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.30 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.5  | All | All | All |

|             |                        |                        |        |     |     |     |
|-------------|------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.7  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.8  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.0.9  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.0  | All | 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> | 6.0.10 | 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> | 6.0.3  | 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> | 6.0.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.7  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.8  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0.9  | All | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |  |
|-----------------------------------|--------|---------|--------------|---------------|--|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |  |

| References                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                                                                                                                   |
| HP-UX update for Apache - Advisories - Secunia                                                                                     |
| HPSBUX02262 SSRT071447 rev. 1 - HP-UX running Apache, Remote Arbitrary Code Execution, Cross Site Scripting (XSS) - c01178795 - HI |
| Sun Solaris 9 Tomcat Multiple Vulnerabilities - Advisories - Secunia                                                               |
| Apache Tomcat Documentation Sample Application Multiple Cross-Site Scripting Vulnerabilities                                       |
| SecurityFocus                                                                                                                      |
| About the security content of Security Update 2008-004 and Mac OS X 10.5.4                                                         |
| Pony Mail!                                                                                                                         |
| Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com                |
| rhn.redhat.com   Red Hat Support                                                                                                   |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                   |
| Apache Tomcat® - Apache Tomcat 4.x vulnerabilities                                                                                 |
| SecurityReason - Tomcat documentation XSS vulnerabilities                                                                          |
| SecurityFocus                                                                                                                      |
| Webmail - OVH                                                                                                                      |

|                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------|
| Repository / Oval Repository                                                                                                                 |
| APPLE-SA-2008-06-30 Security Update 2008-004 and Mac OS X v10.5.4                                                                            |
| sunsolve.sun.com/search/document.do                                                                                                          |
| Friday, January 23, 2009 - Posts - CA Security Response Blog - CA Technologies                                                               |
| Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com                |
| Apache Tomcat - Apache Tomcat 5 vulnerabilities                                                                                              |
| CA Cohesion Application Configuration Manager Apache Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Sec |
| Sun Solaris 10 Tomcat Multiple Vulnerabilities - Advisories - Secunia                                                                        |
| access.redhat.com                                                                                                                            |
| Pony Mail!                                                                                                                                   |
| 404 Not Found                                                                                                                                |
| [SECURITY] Fedora 7 Update: tomcat5-5.5.25-1jpp.1.fc7                                                                                        |
| Pony Mail!                                                                                                                                   |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                             |
| osvdb.org/34875                                                                                                                              |
| Apache Tomcat® - Apache Tomcat 6 vulnerabilities                                                                                             |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                             |
| SecurityFocus                                                                                                                                |
| Fedora update for tomcat5 - Advisories - Secunia                                                                                             |
| IBM X-Force Exchange                                                                                                                         |
| Pony Mail!                                                                                                                                   |
| Pony Mail!                                                                                                                                   |
| Pony Mail!                                                                                                                                   |
| CVE Program record                                                                                                                           |
| NVD vulnerability detail                                                                                                                     |
| <div>◀</div> <div></div> <div>▶</div>                                                                                                        |

No vendor comments have been submitted for this CVE.

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

[site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)