# CVE-2009-0783

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2009-0783 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2009-06-05 16:00:00 UTC |
| **Updated** | 2026-04-23 00:35:47 UTC |
| **Description** | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 permits web applications to replace an |

## Risk And Classification

**Primary CVSS:** v3.0 4.2 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

**Problem Types:** CWE-200 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 4.2 | MEDIUM | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L |
| 2.0 | nvd@nist.gov | Primary | 4.6 | | AV:L/AC:L/Au:N/C:P/I:P/A:P |

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

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

## Vendor Declared Affected Products

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

## References

| Reference | Source |
|---|---|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| '[security bulletin] HPSBUX02579 SSRT100203 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC | af854a3a-2127-42 |
| VMware Products Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-42 |
| SecurityFocus | af854a3a-2127-42 |
| Debian -- Security Information -- DSA-2207-1 tomcat5.5 | af854a3a-2127-42 |
| '[security bulletin] HPSBMA02535 SSRT100029 rev.1 - HP Performance Manager, Remote Unauthorized Acces' - MARC | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| Apache Tomcat® - Apache Tomcat 4.x vulnerabilities | af854a3a-2127-42 |

| | |
|---|---|
| HP-UX update for Tomcat Servlet Engine - Advisories - Community | af854a3a-2127-42 |
| Security Advisories \| Mandriva Linux | af854a3a-2127-42 |
| [SECURITY] Fedora 11 Update: tomcat6-6.0.20-1.fc11 | af854a3a-2127-42 |
| [SECURITY] Fedora 10 Update: tomcat6-6.0.20-1.fc10 | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| IBM X-Force Exchange | af854a3a-2127-42 |
| [Apache-SVN] Revision 781708 | af854a3a-2127-42 |
| '[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC | af854a3a-2127-42 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| SecurityTracker.com Archives - Tomcat Bug Lets Web Applications Access the Files of Other Web Applications | af854a3a-2127-42 |
| Security Advisories \| Mandriva Linux | af854a3a-2127-42 |
| Sun Solaris Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-42 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| SecurityFocus | af854a3a-2127-42 |
| [SECURITY] Fedora 12 Update: tomcat6-6.0.20-1.fc12 | af854a3a-2127-42 |
| APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3 | af854a3a-2127-42 |
| Apache Tomcat XML Parser Information Disclosure Vulnerability | af854a3a-2127-42 |
| Apache Tomcat - Apache Tomcat 5 vulnerabilities | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| [Apache-SVN] Revision 739522 | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| Bug 29936 – XML parser loading problems by container | af854a3a-2127-42 |
| sunsolve.sun.com/search/document.do | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| Security Advisories \| Mandriva Linux | af854a3a-2127-42 |
| [Apache-SVN] Revision 652592 | af854a3a-2127-42 |
| [Apache-SVN] Revision 681156 | af854a3a-2127-42 |
| About the security content of Security Update 2010-002 / Mac OS X v10.6.3 | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| Apache Tomcat® - Apache Tomcat 6 vulnerabilities | af854a3a-2127-42 |
| VMSA-2009-0016.1 | af854a3a-2127-42 |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:012 | af854a3a-2127-42 |

| | |
|---|---|
| [Apache-SVN] Revision 781542 | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| Bug 45933 – Error processing TLD file in webapp with XML parser | af854a3a-2127-42 |
| Pony Mail! | af854a3a-2127-42 |
| 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.