



# CVE-2008-5515

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2008-5515                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2009-06-16 21:00:00 UTC                                                                                                     |
| <b>Updated</b>         | 2023-02-13 02:19:00 UTC                                                                                                     |
| <b>Description</b>     | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalizes th |

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                | Version | Update | Edition | Language |
|-------------|------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.0   | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.1   | 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> | 4.1.11  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.12  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.13  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.14  | 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> | 4.1.16  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.17  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.18  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.19  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.2   | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.20  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.21  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.22  | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.23  | 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> | 4.1.25 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.26 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.27 | 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> | 4.1.29 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.30 | 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> | 4.1.32 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.33 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.34 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.35 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.36 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.37 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.38 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.39 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.10 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.11 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.12 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.13 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.14 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.15 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.16 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.17 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.18 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.19 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.20 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.21 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.22 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.23 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.24 | All | All | All |

|             |                        |                        |        |     |     |     |
|-------------|------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.25 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.26 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.27 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.7  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.8  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.9  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0    | 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> | 6.0.12 | 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> | 6.0.2  | 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> | 6.0.9  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.1  | 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> | 4.1.11 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.12 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.13 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.14 | 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> | 4.1.15 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.16 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.17 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.18 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.19 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.20 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.21 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.22 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.23 | 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> | 4.1.25 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.26 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.27 | 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> | 4.1.29 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.30 | 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> | 4.1.32 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.33 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.34 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.35 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.36 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.37 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.38 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 4.1.39 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.10 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.11 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.12 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.13 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.14 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.15 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.16 | All | All | All |

|             |                        |                        |        |     |     |     |
|-------------|------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.17 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.18 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.19 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.20 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.21 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.22 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.23 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.24 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.25 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.26 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.27 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.7  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.8  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 5.5.9  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Tomcat</a> | 6.0    | 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> | 6.0.12 | 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> | 6.0.2  | 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> | 6.0.9 | All | All | All      |
|                                                                                                               |                        |                        |       |     |     |          |
| References                                                                                                    |                        |                        |       |     |     |          |
| Reference                                                                                                     |                        |                        |       |     |     | Source   |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MISC     |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MISC     |
| '[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC |                        |                        |       |     |     | HP       |
| Repository / Oval Repository                                                                                  |                        |                        |       |     |     | OVAL     |
| Security Advisories   Mandriva Linux                                                                          |                        |                        |       |     |     | MANDRIVA |
| VMware Products Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com   |                        |                        |       |     |     | SECUNIA  |
| Repository / Oval Repository                                                                                  |                        |                        |       |     |     | OVAL     |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MLIST    |
| '[security bulletin] HPSBUX02579 SSRT100203 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC |                        |                        |       |     |     | HP       |
| This page provides Security Information. : Fujitsu Global                                                     |                        |                        |       |     |     | CONFIRM  |
| Apache Tomcat 'RequestDispatcher' Information Disclosure Vulnerability                                        |                        |                        |       |     |     | BID      |
| Repository / Oval Repository                                                                                  |                        |                        |       |     |     | OVAL     |
| 263529                                                                                                        |                        |                        |       |     |     | SUNALERT |
| SUSE Update for Multiple Packages - Advisories - Community                                                    |                        |                        |       |     |     | SECUNIA  |
| SecurityFocus                                                                                                 |                        |                        |       |     |     | BUGTRAQ  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                              |                        |                        |       |     |     | VUPEN    |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MISC     |
| [SECURITY] Fedora 11 Update: tomcat6-6.0.20-1.fc11                                                            |                        |                        |       |     |     | FEDORA   |
| BlackBerry Enterprise Server Multiple Vulnerabilities - Secunia.com                                           |                        |                        |       |     |     | SECUNIA  |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MLIST    |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                              |                        |                        |       |     |     | VUPEN    |
| APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3                                             |                        |                        |       |     |     | APPLE    |
| SecurityFocus                                                                                                 |                        |                        |       |     |     | BUGTRAQ  |
| [SECURITY] Fedora 10 Update: tomcat6-6.0.20-1.fc10                                                            |                        |                        |       |     |     | FEDORA   |
| SecurityFocus                                                                                                 |                        |                        |       |     |     | BUGTRAQ  |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MLIST    |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MISC     |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MLIST    |
| Pony Mail!                                                                                                    |                        |                        |       |     |     | MISC     |
| Debian -- Security Information -- DSA-2207-1 tomcat5.5                                                        |                        |                        |       |     |     | DEBIAN   |
| Apache Tomcat® - Apache Tomcat 4.x vulnerabilities                                                            |                        |                        |       |     |     | CONFIRM  |

|                                                                                                                                   |          |
|-----------------------------------------------------------------------------------------------------------------------------------|----------|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                  | VUPEN    |
| Apache Tomcat - Apache Tomcat 5 vulnerabilities                                                                                   | CONFIRM  |
| Security Advisories   Mandriva Linux                                                                                              | MANDRIVA |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2010:008                                                                | SUSE     |
| Pony Mail!                                                                                                                        | MISC     |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com                                  | SECUNIA  |
| Pony Mail!                                                                                                                        | MLIST    |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:012                                                                | SUSE     |
| Pony Mail!                                                                                                                        | MISC     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                  | VUPEN    |
| [SECURITY] Fedora 12 Update: tomcat6-6.0.20-1.fc12                                                                                | FEDORA   |
| Pony Mail!                                                                                                                        | MLIST    |
| Sun Solaris Tomcat Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com                        | SECUNIA  |
| Security Advisories   Mandriva Linux                                                                                              | MANDRIVA |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                  | VUPEN    |
| VMSA-2009-0016.1                                                                                                                  | CONFIRM  |
| Fujitsu Interstage Products Information Disclosure Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com | SECUNIA  |
| HP-UX update for Tomcat Servlet Engine - Advisories - Community                                                                   | SECUNIA  |
| JVN#63832775 Apache Tomcat information disclosure vulnerability                                                                   | JVN      |
| About the security content of Security Update 2010-002 / Mac OS X v10.6.3                                                         | CONFIRM  |
| '[security bulletin] HPSBMA02535 SSRT100029 rev.1 - HP Performance Manager, Remote Unauthorized Acces' - MARC                     | HP       |
| Apache Tomcat® - Apache Tomcat 6 vulnerabilities                                                                                  | CONFIRM  |
| Pony Mail!                                                                                                                        | MLIST    |
| 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.

© [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 registered 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](#).

**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)