



# CVE-2013-4152

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

## Summary

|                        |                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-4152                                                                                                        |
| <b>State</b>           | PUBLIC                                                                                                               |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                         |
| <b>Published</b>       | 2014-01-23 21:55:00 UTC                                                                                              |
| <b>Updated</b>         | 2022-04-11 17:36:00 UTC                                                                                              |
| <b>Description</b>     | The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disat |

## Risk And Classification

### Problem Types: CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                       | Product                          | Version  | Update | Edition | Language |
|-------------|------------------------------|----------------------------------|----------|--------|---------|----------|
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | m1     | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | m2     | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | m3     | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | m4     | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | rc1    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | rc2    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0    | rc3    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0.m1 | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.0.m2 | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.1    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.2    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.3    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.4    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.5    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.6    | All    | All     | All      |
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | 3.0.7    | All    | All     | All      |

[illegible]

|             |                              |                                  |       |            |     |     |
|-------------|------------------------------|----------------------------------|-------|------------|-----|-----|
| Application | <a href="#">Springsource</a> | <a href="#">Spring Framework</a> | All   | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.0.6 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.0.7 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.1.0 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.1.1 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.1.2 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.1.3 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.1.4 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.2.0 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.2.1 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 3.2.2 | All        | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | 4.0.0 | milestone1 | All | All |
| Application | <a href="#">Vmware</a>       | <a href="#">Spring Framework</a> | All   | All        | All | All |

| References                                                                                                                    |  |  |  |  |          |  |
|-------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|----------|--|
| Reference                                                                                                                     |  |  |  |  | Source   |  |
| About Secunia Research   Flexera                                                                                              |  |  |  |  | SECUNIA  |  |
| Red Hat Customer Portal                                                                                                       |  |  |  |  | REDHAT   |  |
| Spring Framework CVE-2013-4152 Multiple XML External Entity Injection Vulnerabilities                                         |  |  |  |  | BID      |  |
| Added 'processExternalEntities' to JAXB2Marshaller by poutsma · Pull Request #317 · spring-projects/spring-framework · GitHub |  |  |  |  | CONFIRM  |  |
| CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework   GoPivotal                                             |  |  |  |  | CONFIRM  |  |
| Fix potential security risk when using Spring OXM [SPR-10806] · Issue #15432 · spring-projects/spring-framework · GitHub      |  |  |  |  | CONFIRM  |  |
| Debian -- Security Information -- DSA-2842-1 libspring-java                                                                   |  |  |  |  | DEBIAN   |  |
| Bugtraq: CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework                                                |  |  |  |  | BUGTRAC  |  |
| Full Disclosure: XXE Injection in Spring Framework                                                                            |  |  |  |  | FULLDISC |  |
| Red Hat Customer Portal                                                                                                       |  |  |  |  | REDHAT   |  |
| Red Hat Customer Portal                                                                                                       |  |  |  |  | REDHAT   |  |
| Security Advisory SA56247 - Debian update for libspring-java - Secunia                                                        |  |  |  |  | SECUNIA  |  |
| Red Hat Customer Portal                                                                                                       |  |  |  |  | REDHAT   |  |
| 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)