

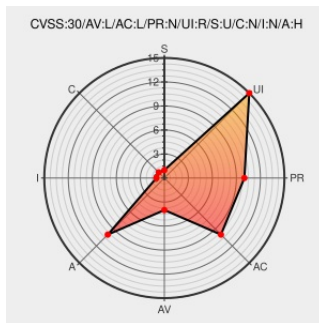


CVE-2015-3192

Published on: 07/12/2016 12:00:00 AM UTC

Last Modified on: 04/11/2022 05:18:00 PM UTC

CVE-2015-3192

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

Pivotal Spring Framework before 3.2.14 and 4.x before 4.1.7 do not properly process inline DTD declarations when DTD is not entirely disabled, which allows remote attackers to cause a denial of service (memory consumption and out-of-memory errors) via a crafted XML file.

CVE-2015-3192 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2016:1219
Red Hat Customer Portal	web.archive.org	REDHAT RHSA-2016:2036

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2035
[SECURITY] [DLA 1853-1] libspring-java security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20190713 [SECURITY] [DLA 1853-1] libspring-java security update
Red Hat JBoss XML Parsing Flaw Lets Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036587
CVE-2015-3192 - DoS Attack with XML Input Security Pivotal	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM pivotal.io/security/cve-2015-3192
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2016:1218
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1592
[SPR-13136] XML input vulnerability based on DTD declaration - Spring JIRA	jira.spring.io text/html	CONFIRM jira.spring.io/browse/SPR-13136
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1593
[SECURITY] Fedora 21 Update: springframework-3.2.14-1.fc21	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-11184
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2035
Spring Framework CVE-2015-3192 Denial-Of-Service Vulnerability	cve.report (archive) text/html	BID 90853
[SECURITY] Fedora 22 Update: springframework-3.2.14-1.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-11165
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

Related QID Numbers

981250 Java (maven) Security Update for org.springframework:spring-core (GHSA-6v7w-535j-rq5m)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All

Operating System	Fedora project	Fedora	22	All	All	All
Application	Pivotal Software	Spring Framework	3.2.0	All	All	All
Application	Pivotal Software	Spring Framework	3.2.1	All	All	All
Application	Pivotal Software	Spring Framework	3.2.10	All	All	All
Application	Pivotal Software	Spring Framework	3.2.11	All	All	All
Application	Pivotal Software	Spring Framework	3.2.12	All	All	All
Application	Pivotal Software	Spring Framework	3.2.13	All	All	All
Application	Pivotal Software	Spring Framework	3.2.2	All	All	All
Application	Pivotal Software	Spring Framework	3.2.3	All	All	All
Application	Pivotal Software	Spring Framework	3.2.4	All	All	All
Application	Pivotal Software	Spring Framework	3.2.5	All	All	All
Application	Pivotal Software	Spring Framework	3.2.6	All	All	All
Application	Pivotal Software	Spring Framework	3.2.7	All	All	All
Application	Pivotal Software	Spring Framework	3.2.8	All	All	All
Application	Pivotal Software	Spring Framework	3.2.9	All	All	All
Application	Pivotal Software	Spring Framework	4.1.0	All	All	All
Application	Pivotal Software	Spring Framework	4.1.1	All	All	All
Application	Pivotal Software	Spring Framework	4.1.2	All	All	All
Application	Pivotal Software	Spring Framework	4.1.3	All	All	All
Application	Pivotal Software	Spring Framework	4.1.4	All	All	All
Application	Pivotal Software	Spring Framework	4.1.5	All	All	All
Application	Pivotal Software	Spring Framework	4.1.6	All	All	All
Application	Pivotal Software	Spring Framework	3.2.0	All	All	All
Application	Pivotal Software	Spring Framework	3.2.1	All	All	All
Application	Pivotal Software	Spring Framework	3.2.10	All	All	All
Application	Pivotal Software	Spring Framework	3.2.11	All	All	All
Application	Pivotal Software	Spring Framework	3.2.12	All	All	All
Application	Pivotal Software	Spring Framework	3.2.13	All	All	All
Application	Pivotal Software	Spring Framework	3.2.2	All	All	All
Application	Pivotal Software	Spring Framework	3.2.3	All	All	All
Application	Pivotal Software	Spring Framework	3.2.4	All	All	All
Application	Pivotal Software	Spring Framework	3.2.5	All	All	All
Application	Pivotal Software	Spring Framework	3.2.6	All	All	All
Application	Pivotal Software	Spring Framework	3.2.7	All	All	All
Application	Pivotal Software	Spring Framework	3.2.8	All	All	All

Application	Pivotal Software	Spring Framework	3.2.9	All	All	All
Application	Pivotal Software	Spring Framework	4.1.0	All	All	All
Application	Pivotal Software	Spring Framework	4.1.1	All	All	All
Application	Pivotal Software	Spring Framework	4.1.2	All	All	All
Application	Pivotal Software	Spring Framework	4.1.3	All	All	All
Application	Pivotal Software	Spring Framework	4.1.4	All	All	All
Application	Pivotal Software	Spring Framework	4.1.5	All	All	All
Application	Pivotal Software	Spring Framework	4.1.6	All	All	All
Application	Vmware	Spring Framework	3.2.1	All	All	All
Application	Vmware	Spring Framework	3.2.10	All	All	All
Application	Vmware	Spring Framework	3.2.11	All	All	All
Application	Vmware	Spring Framework	3.2.12	All	All	All
Application	Vmware	Spring Framework	3.2.13	All	All	All
Application	Vmware	Spring Framework	3.2.2	All	All	All
Application	Vmware	Spring Framework	3.2.3	All	All	All
Application	Vmware	Spring Framework	3.2.4	All	All	All
Application	Vmware	Spring Framework	3.2.5	All	All	All
Application	Vmware	Spring Framework	3.2.6	All	All	All
Application	Vmware	Spring Framework	3.2.7	All	All	All
Application	Vmware	Spring Framework	3.2.8	All	All	All
Application	Vmware	Spring Framework	3.2.9	All	All	All
Application	Vmware	Spring Framework	4.1.1	All	All	All
Application	Vmware	Spring Framework	4.1.2	All	All	All
Application	Vmware	Spring Framework	4.1.3	All	All	All
Application	Vmware	Spring Framework	4.1.4	All	All	All
Application	Vmware	Spring Framework	4.1.5	All	All	All
Application	Vmware	Spring Framework	4.1.6	All	All	All
cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:						
cpe:2.3:a:pivotal_software:spring_framework:3.2.0:*:*:*:*:*:						
cpe:2.3:a:pivotal_software:spring_framework:3.2.1:*:*:*:*:*:						
cpe:2.3:a:pivotal_software:spring_framework:3.2.10:*:*:*:*:*:						

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.11:::*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.12:::*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.13:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.2:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.3:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.4:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.5:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.6:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.7:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.8:*:*:*:*:*
```

cpe:2.3:a:pivotal_software:spring_framework:3.2.9:*:*:*:*:*:

```
cpe:2.3:a:pivotal software:spring framework:4.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.1:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal software:spring framework:4.1.2:*:*:*:*:*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.3:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.4:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.5:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:4.1.6:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.0:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.1:*:*:*:*:*
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.10:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.11:::*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.12:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.13:::*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.2:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.3:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.4:*:*:*:*:*
```

```
cpe:2.3:a:pivotal software:spring framework:3.2.5:*:*:*:*:*
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.6:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.7:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.8:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:3.2.9:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.1:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.2:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.3:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.4:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.1.6:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.3:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.4.*:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:3.2.9:*:*:*:*:*:*:*
```

```
cpe:2.3:a:vmware:spring_framework:4.1.1:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:4.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:4.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:4.1.4:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:spring_framework:4.1.5:*:*:*:*:*:*
```

cpe:2.3:a:vmware:spring_framework:4.1.6:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

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