

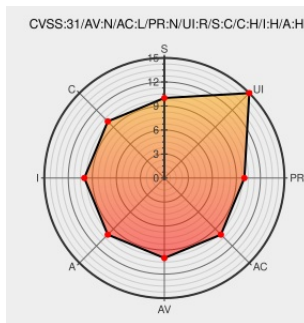


CVE-2015-5211

Published on: 05/25/2017 12:00:00 AM UTC

Last Modified on: 06/05/2022 03:44:00 AM UTC

CVE-2015-5211

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

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Under some situations, the Spring Framework 4.2.0 to 4.2.1, 4.0.0 to 4.1.7, 3.2.0 to 3.2.14 and older unsupported versions is vulnerable to a Reflected File Download (RFD) attack. The attack involves a malicious user crafting a URL with a batch script extension that results in the response being downloaded rather than rendered and also includes some input reflected in the response.

CVE-2015-5211 has been assigned by [secure@de11.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **9.3 - HIGH**

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

CVE References

Description	Tags	Link
[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

Reflected File Download - A New Web Attack Vector	Exploit Technical Description www.trustwave.com text/html	 MISC www.trustwave.com/Resources/SpiderLabs-Blog/Reflected-File-Download---A-New-Web-Attack-Vector/
CVE-2015-5211 RFD Attack in Spring Framework Security Pivotal	Vendor Advisory pivotal.io text/html	 CONFIRM pivotal.io/security/cve-2015-5211

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

980959 Java (maven) Security Update for org.springframework:spring-core (GHSA-pgf9-h69p-pcgf)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	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	3.2.14	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	4.0.0	All	All	All
Application	Pivotal Software	Spring Framework	4.0.1	All	All	All
Application	Pivotal Software	Spring Framework	4.0.2	All	All	All
Application	Pivotal Software	Spring Framework	4.0.3	All	All	All
Application	Pivotal Software	Spring Framework	4.0.4	All	All	All

Application	Pivotal Software	Spring Framework	4.0.5	All	All	All
Application	Pivotal Software	Spring Framework	4.0.6	All	All	All
Application	Pivotal Software	Spring Framework	4.0.7	All	All	All
Application	Pivotal Software	Spring Framework	4.0.8	All	All	All
Application	Pivotal Software	Spring Framework	4.0.9	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	4.1.7	All	All	All
Application	Pivotal Software	Spring Framework	4.2.0	All	All	All
Application	Pivotal Software	Spring Framework	4.2.1	All	All	All
Application	Vmware	Spring Framework	3.2.0	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	3.2.14	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	4.0.0	All	All	All
Application	Vmware	Spring Framework	4.0.1	All	All	All
Application	Vmware	Spring Framework	4.0.2	All	All	All
Application	Vmware	Spring Framework	4.0.3	All	All	All
Application	Vmware	Spring Framework	4.0.4	All	All	All
Application	Vmware	Spring Framework	4.0.5	All	All	All

Application	Vmware	Spring Framework	4.0.6	All	All	All
Application	Vmware	Spring Framework	4.0.7	All	All	All
Application	Vmware	Spring Framework	4.0.8	All	All	All
Application	Vmware	Spring Framework	4.0.9	All	All	All
Application	Vmware	Spring Framework	4.1.0	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
Application	Vmware	Spring Framework	4.1.7	All	All	All
Application	Vmware	Spring Framework	4.2.0	All	All	All
Application	Vmware	Spring Framework	4.2.1	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
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:3.2.14:*****:						
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:4.0.0:*****:						

cpe:2.3:a:pivotal_software:spring_framework:4.0.1:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.2:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.3:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.4:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.5:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.6:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.7:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.8:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.0.9:*****:*
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:4.1.7:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.2.0:*****:*
cpe:2.3:a:pivotal_software:spring_framework:4.2.1:*****:*
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:3.2.14:*****:*
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:3.2.4:::~::~~::~~::~::
```

```
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:4.0.0:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.2:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal:software:spring:framework:4.0.3:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.4:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.5:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.7:*:*:*:*:*:*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.8:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.0.9:*:*:*:*:*.*
```

```
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:4.1.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:pivotal software:spring framework:4.2.0:*:*:*:*:*.*
```

```
cpe:2.3:a:pivotal_software:spring_framework:4.2.1:*:*:*:*:*.*
```

```
cpe:2.3:a:vmware:spring_framework:3.2.0:*:*:*:*:*:*
```

```
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:3.2.14:*****:
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:4.0.0:*****:
cpe:2.3:a:vmware:spring_framework:4.0.1:*****:
cpe:2.3:a:vmware:spring_framework:4.0.2:*****:
cpe:2.3:a:vmware:spring_framework:4.0.3:*****:
cpe:2.3:a:vmware:spring_framework:4.0.4:*****:
cpe:2.3:a:vmware:spring_framework:4.0.5:*****:
cpe:2.3:a:vmware:spring_framework:4.0.6:*****:
cpe:2.3:a:vmware:spring_framework:4.0.7:*****:
cpe:2.3:a:vmware:spring_framework:4.0.8:*****:
cpe:2.3:a:vmware:spring_framework:4.0.9:*****:
cpe:2.3:a:vmware:spring_framework:4.1.0:*****:
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:*****:
cpe:2.3:a:vmware:spring_framework:4.1.7:*****:
cpe:2.3:a:vmware:spring_framework:4.2.0:*****:
cpe:2.3:a:vmware:spring_framework:4.2.1:*****:

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](#)