



CVE-2015-0201

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

Summary

CVE	CVE-2015-0201
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-10 14:59:00 UTC
Updated	2022-04-11 17:18:00 UTC
Description	The Java SockJS client in Pivotal Spring Framework 4.1.x before 4.1.5 generates predictable session ids, which allows remote attackers to hijack sessions and execute arbitrary code.

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	4.1.0	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	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

References

Reference	Source	Link	Tags
-----------	--------	------	------

CVE-2015-0201 Insufficiently random session id in Java SockJS client Security Pivotal	CONFIRM	pivotal.io	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
No vendor comments have been submitted for this CVE.			
Legacy QID Mappings			
981330 Java (maven) Security Update for org.springframework:spring-core (GHSA-45vg-2v73-vm62)			

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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