

CVE-2016-5007

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2016-5007
State	PUBLISHED
Assigner	dell
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-25 17:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Both Spring Security 3.2.x, 4.0.x, 4.1.0 and the Spring Framework 3.2.x, 4.0.x, 4.1.x, 4.2.x rely on URL pattern mappings fo

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Problem Types: CWE-264 | Security Control Bypass

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Spring Framework	3.2.0	All	All	All
Application	Pivotal Software	Spring Framework	4.0.0	All	All	All
Application	Pivotal Software	Spring Framework	4.1.0	All	All	All
Application	Pivotal Software	Spring Framework	4.2.0	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	3.2.15	All	All	All
Application	Vmware	Spring Framework	3.2.16	All	All	All
Application	Vmware	Spring Framework	3.2.17	All	All	All
Application	Vmware	Spring Framework	3.2.18	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	4.0.1	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	4.1.1	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	4.1.8	All	All	All
Application	Vmware	Spring Framework	4.1.9	All	All	All
Application	Vmware	Spring Framework	4.2.1	All	All	All
Application	Vmware	Spring Framework	4.2.2	All	All	All
Application	Vmware	Spring Framework	4.2.3	All	All	All
Application	Vmware	Spring Framework	4.2.4	All	All	All
Application	Vmware	Spring Framework	4.2.5	All	All	All
Application	Vmware	Spring Framework	4.2.6	All	All	All
Application	Vmware	Spring Framework	4.2.7	All	All	All
Application	Vmware	Spring Framework	4.2.8	All	All	All
Application	Vmware	Spring Framework	4.2.9	All	All	All
Application	Vmware	Spring Security	3.2.0	All	All	All
Application	Vmware	Spring Security	3.2.1	All	All	All
Application	Vmware	Spring Security	3.2.10	All	All	All
Application	Vmware	Spring Security	3.2.2	All	All	All

Application	Vmware	Spring Security	3.2.2	All	All	All
Application	Vmware	Spring Security	3.2.3	All	All	All
Application	Vmware	Spring Security	3.2.4	All	All	All
Application	Vmware	Spring Security	3.2.5	All	All	All
Application	Vmware	Spring Security	3.2.6	All	All	All
Application	Vmware	Spring Security	3.2.7	All	All	All
Application	Vmware	Spring Security	3.2.8	All	All	All
Application	Vmware	Spring Security	3.2.9	All	All	All
Application	Vmware	Spring Security	4.0.0	All	All	All
Application	Vmware	Spring Security	4.0.1	All	All	All
Application	Vmware	Spring Security	4.0.2	All	All	All
Application	Vmware	Spring Security	4.0.3	All	All	All
Application	Vmware	Spring Security	4.0.4	All	All	All
Application	Vmware	Spring Security	4.1.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Pivotal	Spring Security	affected 3.2.x		Not specified	
CNA	Pivotal	Spring Security	affected 4.0.x		Not specified	
CNA	Pivotal	Spring Security	affected 4.1.0		Not specified	
CNA	Pivotal	Spring Framework	affected 3.2.x		Not specified	
CNA	Pivotal	Spring Framework	affected 4.0.x		Not specified	
CNA	Pivotal	Spring Framework	affected 4.1.x		Not specified	
CNA	Pivotal	Spring Framework	affected 4.2.x		Not specified	
CNA	Pivotal	Spring Framework	affected older unsupported versions are also affected		Not specified	

References			
Reference	Source		Link
Oracle Critical Patch Update - July 2019	af854a3a-2127-422b-91ae-364da2661108		www.c
Spring Security and Spring Framework CVE-2016-5007 Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.s
Oracle Critical Patch Update - April 2018	af854a3a-2127-422b-91ae-364da2661108		www.c
CVE-2016-5007 Spring Security / MVC Path Matching Inconsistency Security Pivotal	af854a3a-2127-422b-91ae-364da2661108		pivota
CVE Program record	CVE.ORG		www.c
NVD vulnerability detail	NVD		nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981205](#) Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-8crv-49fr-2h6j)

© [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](#)