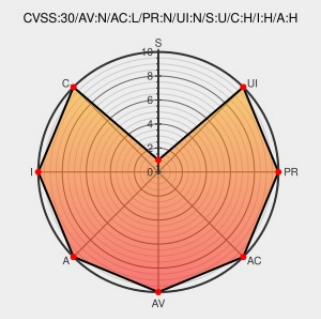
CVE-2014-3527

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

Last Modified on: 06/08/2021 06:22:00 PM UTC

CVE-2014-3527

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Spring Security from Pivotal Software contain the following vulnerability:

When using the CAS Proxy ticket authentication from Spring Security 3.1 to 3.2.4 a malicious CAS Service could trick another CAS Service into authenticating a proxy ticket that was not associated. This is due to the fact that the proxy ticket authentication uses the information from the HttpServletRequest which is populated based upon untrusted information within the HTTP request. This means if there are access control restrictions on which CAS services can authenticate to one another, those restrictions can be bypassed. If users are not using CAS Proxy tickets and not basing access control decisions based upon the CAS Service, then there is no impact to users.

CVE-2014-3527 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Pivotal** - **Spring Security** version **3.1 to 3.2.4**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2014-3527 Access Control Bypass in Spring Security | Security | Pivotal	Vendor Advisory pivotal.io text/html	CONFIRM pivotal.io/security/cve-2014-3527

Related QID Numbers

980545 Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-wmv4-5w76-vp9g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Spring Security	3.1.0	All	All	All
Application	Pivotal Software	Spring Security	3.1.1	All	All	All
Application	Pivotal Software	Spring Security	3.1.2	All	All	All
Application	Pivotal Software	Spring Security	3.1.3	All	All	All
Application	Pivotal Software	Spring Security	3.1.4	All	All	All
Application	Pivotal Software	Spring Security	3.2.0	All	All	All
Application	Pivotal Software	Spring Security	3.2.1	All	All	All
Application	Pivotal Software	Spring Security	3.2.2	All	All	All
Application	Pivotal Software	Spring Security	3.2.3	All	All	All
Application	Pivotal Software	Spring Security	3.2.4	All	All	All
Application	Pivotal Software	Spring Security	3.1.0	All	All	All
Application	Pivotal Software	Spring Security	3.1.1	All	All	All
Application	Pivotal Software	Spring Security	3.1.2	All	All	All
Application	Pivotal Software	Spring Security	3.1.3	All	All	All
Application	Pivotal Software	Spring Security	3.1.4	All	All	All
Application	Pivotal Software	Spring Security	3.2.0	All	All	All
Application	Pivotal Software	Spring Security	3.2.1	All	All	All
Application	Pivotal Software	Spring Security	3.2.2	All	All	All
Application	Pivotal Software	Spring Security	3.2.3	All	All	All
Application	Pivotal Software	Spring Security	3.2.4	All	All	All
Application	Vmware	Spring Security	3.1.0	All	All	All
Application	Vmware	Spring Security	3.1.1	All	All	All

Application	Vmware	Spring Security	3.1.2	All	All	All
Application	Vmware	Spring Security	3.1.3	All	All	All
Application	Vmware	Spring Security	3.1.4	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	3.2.2	All	All	All
Application	Vmware	Spring Security	3.2.3	All	All	All
Application	Vmware	Spring Security	3.2.4	All	All	All

cpe:2.3:a:pivotal_software:spring_security:3.1.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.3:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.4:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.3:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.4:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.3:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.1.4:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.3:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring_security:3.2.4:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.1.0:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.1.1:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.1.2:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.1.3:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.1.4:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.2.0:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.2.1:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.2.2:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.2.3:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_security:3.2.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→