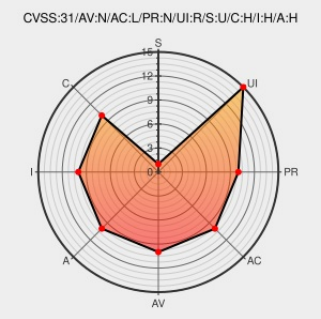
CVE-2015-5258

Published on: 08/22/2017 12:00:00 AM UTC

Last Modified on: 06/09/2021 04:20:00 PM UTC

CVE-2015-5258

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in springframework-social before 1.1.3.

CVE-2015-5258 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 23 Update: springframework-social-1.0.3-3.fc23	Third Party Advisory, lists.fedoraproject.org, text/html	FEDORA FEDORA-2016-4d0e6ba888
Bug 1305443 – CVE-2015-5258 springframework-social: CSRF vulnerability	Issue Tracking	CONFIRM

when authorizing an app against OAuth 2 API provider	Third Party Advisory VDB Entry bugzilla.redhat.com text/html	bugzilla.redhat.com/show_bug.cgi?id=1305443

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Pivotal Software	Spring Social	1.1.2	All	All	All
Application	Pivotal Software	Spring Social	1.1.2	All	All	All
Application	Vmware	Spring Social	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring_social:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring_social:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:spring_social:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→