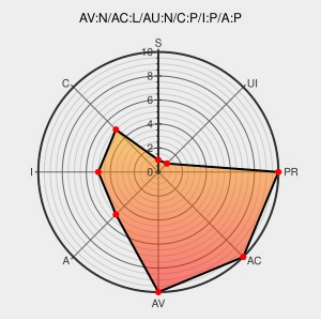
CVE-2015-5325

Published on: 11/25/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5325

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



Certain versions of Jenkins from Jenkins contain the following vulnerability:

Jenkins before 1.638 and LTS before 1.625.2 allow attackers to bypass intended slave-to-master access restrictions by leveraging a JNLP slave. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-3665.

CVE-2015-5325 has been assigned by secalert@redhat.com to track the vulnerability

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
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2016:0070
Jenkins Security Advisory 2015-11-11 - Security Advisories - Jenkins Wiki	Vendor Advisory wiki.jenkins-ci.org text/html	CONFIRM wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2015-11-11
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0489

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Jenkins	All	All	All	All
Application	Jenkins	Jenkins	All	All	All	All
Application	Redhat	Openshift	2.0	All	All	All
Application	Redhat	Openshift	2.0	All	All	All
Application	Redhat	Openshift	All	All	All	All

cpe:2.3:a:jenkins:jenkins:*:*:*:*:lts:*:*:*:

cpe:2.3:a:jenkins:jenkins:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift:*:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→