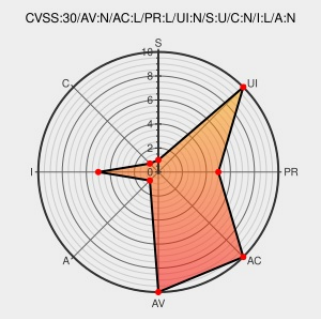
CVE-2016-3725

Published on: 05/17/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:03 PM UTC

CVE-2016-3725

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



Certain versions of Jenkins from Jenkins contain the following vulnerability:

Jenkins before 2.3 and LTS before 1.651.2 allows remote authenticated users to trigger updating of update site metadata by leveraging a missing permissions check. NOTE: this issue can be combined with DNS cache poisoning to cause a denial of service (service disruption).

CVE-2016-3725 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1773

Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2016:1206
Jenkins Security Advisory 2016-05-11 - Security Advisories - Jenkins Wiki	Vendor Advisory wiki.jenkins-ci.org text/html	CONFIRM wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-05-11
Jenkins Security Advisory 2016-05-11 | CloudBees	Vendor Advisory www.cloudbees.com text/html	CONFIRM www.cloudbees.com/jenkins-security-advisory-2016-05-11

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	3.1	All	All	All
Application	Redhat	Openshift	3.2	All	All	All
Application	Redhat	Openshift	3.1	All	All	All
Application	Redhat	Openshift	3.2	All	All	All

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

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

cpe:2.3:a:redhat:openshift:3.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:redhat:openshift:3.2:*:*:*:enterprise:*:*:*:

cpe:2.3:a:redhat:openshift:3.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:redhat:openshift:3.2:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report