



CVE-2014-3679

Published on: 10/16/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

CVE-2014-3679

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Monitoring Plugin](#) from [Jenkins-ci](#) contain the following vulnerability:

The Monitoring plugin before 1.53.0 for Jenkins allows remote attackers to obtain sensitive information by accessing unspecified pages.

CVE-2014-3679 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Monitoring - Jenkins - Jenkins Wiki

[Vendor Advisory](#)
[wiki.jenkins-ci.org](#)
[text/html](#)

CONFIRM wiki.jenkins-ci.org/display/JENKINS/Monitoring

Jenkins Security Advisory 2014-10-01 - Security Advisories - Jenkins Wiki

[Vendor Advisory](#)
[wiki.jenkins-ci.org](#)
[text/html](#)

CONFIRM wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2014-10-01

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

cpe:2.3:a:jenkins-ci:monitoring_plugin:1.44.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.45.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.46.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.47.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.48.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.49.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.50.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.51.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.52.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.40.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.41.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.42.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.43.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.44.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.45.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.46.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.47.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.48.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.49.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.50.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.51.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:1.52.0:*:*:*:*:cloudbees_jenkins:*:*:
cpe:2.3:a:jenkins-ci:monitoring_plugin:*:*:*:*:*:cloudbees_jenkins:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)