

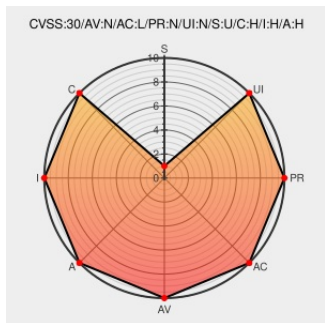


CVE-2017-1000362

Published on: 07/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000362

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Jenkins](#) from [Jenkins](#) contain the following vulnerability:

The re-key admin monitor was introduced in Jenkins 1.498 and re-encrypted all secrets in JENKINS_HOME with a new key. It also created a backup directory with all old secrets, and the key used to encrypt them. These backups were world-readable and not removed afterwards. Jenkins now deletes the backup directory, if present.

Upgrading from before 1.498 will no longer create a backup directory. Administrators relying on file access permissions in their manually created backups are advised to check them for the directory \$JENKINS_HOME/jenkins.security.RekeySecretAdminMonitor/backups, and delete it if present.

CVE-2017-1000362 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Jenkins Security Advisory 2017-02-01	Vendor Advisory jenkins.io text/html	 CONFIRM jenkins.io/security/advisory/2017-02-01/

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Jenkins	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →