



CVE-2017-2604

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-2604
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-15 21:29:00 UTC
Updated	2019-10-09 23:26:00 UTC
Description	In Jenkins before versions 2.44, 2.32.2 low privilege users were able to act on administrative monitors due to them not being properly authenticated.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Jenkins CVE-2017-2604 Privilege Escalation Vulnerability	BID	www.bidsa.org
Bug 1418714 – CVE-2017-2604 jenkins: Low privilege users were able to act on administrative monitors (SECURITY-371)	CONFIRM	bugzilla.redhat.com/bug/1418714
Merge pull request #85 from jenkinsci-cert/security-371-staplerproxy · jenkinsci/jenkins@6efcf6c · GitHub	CONFIRM	github.com/jenkinsci/jenkins/pull/85
Jenkins Security Advisory 2017-02-01	CONFIRM	jenkins.org/security/2017-02-01
CVE Program record	CVE.ORG	cve.org/cve/2017/2604
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2017-2604

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API [cve.report/api](#)

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