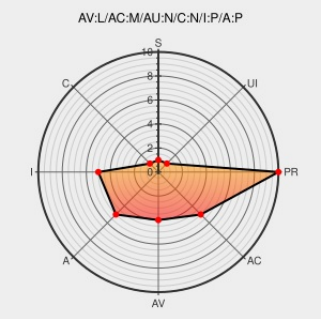
CVE-2013-4260

Published on: 09/16/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:45:00 AM UTC

CVE-2013-4260

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



Certain versions of Ansible from Redhat contain the following vulnerability:

lib/ansible/playbook/__init__.py in Ansible 1.2.x before 1.2.3, when playbook does not run due to an error, allows local users to overwrite arbitrary files via a symlink attack on a retry file with a predictable name in /var/tmp/ansible/.

CVE-2013-4260 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.3 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
998227 – (CVE-2013-4260) CVE-2013-4260 ansible: predictible filename used for failed result in world writable directory	Issue Tracking, Patch, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=998227
Redirecting to Google Groups	groups.google.com, text/html	MISC groups.google.com/forum/#%21topic/ansible-project/UVDYW0HGcNg
IBM X-Force Exchange	VDB Entry, Vendor Advisory, exchange.xforce.ibmcloud.com, text/html	XF ansible-cve20134260-symlink(86898)
Ansible Privacy Policy	Vendor Advisory, www.ansible.com, text/html	CONFIRM www.ansible.com/security

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	Redhat	Ansible	1.2	All	All	All
Application	Redhat	Ansible	1.2.1	All	All	All
Application	Redhat	Ansible	1.2.2	All	All	All
Application	Redhat	Ansible	1.2	All	All	All
Application	Redhat	Ansible	1.2.1	All	All	All
Application	Redhat	Ansible	1.2.2	All	All	All

cpe:2.3:a:redhat:ansible:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:1.2.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→