CVE-2016-3096

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-3096
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-03 14:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The create_script function in the lxc_container module in Ansible before 1.9.6-1 and 2.x before 2.0.2.0 allows local users to

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-59 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Application	Redhat	Ansible	2.0	All	All	All
Application	Redhat	Ansible	2.0.1	All	All	All
Application	Redhat	Ansible	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
ansible/CHANGELOG.md at v1.9.6-1 · ansible/ansible · GitHub	af854a3a-21
[SECURITY] Fedora 22 Update: ansible-2.0.2.0-1.fc22	af854a3a-21
[SECURITY] Fedora 24 Update: ansible-2.0.2.0-1.fc24	af854a3a-21
do not use a predictable filenames in the LXC plugin by evgeni · Pull Request #1941 · ansible/ansible-modules-extras · GitHub	af854a3a-21
[SECURITY] Fedora 23 Update: ansible-2.0.2.0-1.fc23	af854a3a-21

1322925 – (CVE-2016-3096) CVE-2016-3096 ansible: Code execution vulnerability in lxc_container	af854a3a-21
[SECURITY] Fedora 22 Update: ansible1.9-1.9.6-1.fc22	af854a3a-21
do not use a predictable filenames in the LXC plugin by evgeni · Pull Request #1941 · ansible/ansible-modules-extras · GitHub	af854a3a-21
Ansible: Privilege escalation (GLSA 201607-14) — Gentoo security	af854a3a-21
Google Groups	af854a3a-21
Google Groups	af854a3a-21
[SECURITY] Fedora 23 Update: ansible1.9-1.9.6-1.fc23	af854a3a-21
ansible/CHANGELOG.md at v2.0.2.0-1 · ansible/ansible · GitHub	af854a3a-21
Google Groups	MITRE
Google Groups	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980882 Python (pip) Security Update for ansible (GHSA-rh6x-qvg7-rrmj)