Ansible-lightspeed: broken object level authorization leading to cross-user ai conversation context injection in ansible lightspeed api

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

Summary

CVE	CVE-2026-0598
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-06 06:15:49 UTC
Updated	2026-05-04 22:16:18 UTC
Description	A security flaw was identified in the Ansible Lightspeed API conversation endpoints that handle AI chat interactions. The AF

Risk And Classification

Primary CVSS: v3.1 4.2 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

EPSS: 0.000120000 probability, percentile 0.016880000 (date 2026-05-05)

Problem Types: CWE-283 | CWE-283 Unverified Ownership

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6	unaffected 1777387242 * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified

CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:13545	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-0598	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Laura Pardo (RedHat) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-05T07:34:33.335Z	Reported to Red Hat.
CNA	2026-02-06T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**