Bug 2427094 (CVE-2026-0598) - CVE-2026-0598 ansible-lightspeed: Broken Object Level Authorization Leading to Cross-User AI Conversation Context Injection in Ansible Lightspeed API

Keywords:	Security
Status:	NEW
Alias:	CVE-2026-0598
Deadline:	2026-02-06
Product:	Security Response
Component:	vulnerability
Version:	unspecified
Hardware:	All
OS:	Linux
Priority:	medium
Severity:	medium
Target Milestone:	---
Assignee:	Product Security DevOps Team
QA Contact:	
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	
Blocks:	
TreeView+	depends on / blocked

Reported:	2026-01-05 07:48 UTC by OSIDB Bzimport
Modified:	2026-02-06 05:45 UTC (History)
CC List:	25 users (show)
Fixed In Version:	
Clone Of:	
Environment:	
Last Closed:	
Embargoed:	

Attachments (Terms of Use)

OSIDB Bzimport 2026-01-05 07:48:13 UTC Description

```
Broken Object Level Authorization (BOLA) vulnerability in the
Ansible Lightspeed AI conversation endpoints. The flaw occurs
due to missing ownership validation of the conversation_id
parameter in the /api/v0/ai/chat/, /api/v1/ai/chat/, and
streaming chat APIs. Although UUIDs are used, the backend does
not verify that the authenticated user owns the referenced
conversation, and conversations are incorrectly mapped to a
default null user ID. An authenticated attacker who obtains a
valid conversation identifier can access prior conversation
history and inject new prompts into another user’s AI session,
potentially influencing generated Ansible playbooks. This can
```

be exploited remotely without user interaction and leads to unauthorized information disclosure and integrity compromise.

Note

You need to log in before you can comment on or make changes to this bug.