INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:21 UTC

CVE-2026-12515: Katello Missing Authorization Enables Repository Information Disclosure in Red Hat Satellite

CVE VULNERABILITY | MEDIUM | CVSS 4.3

SCC Item ID	SCC-CVE-2026-0333
Type	CVE Vulnerability
CVE ID	CVE-2026-12515
Severity	MEDIUM
CVSS Base Score	4.3
Affected Products	Katello (Red Hat Satellite), specific version range not confirmed from available sources
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

A missing authorization flaw in Katello, a core component of Red Hat Satellite, allows authenticated users with limited repository permissions to read content metadata from repositories outside their authorized scope. The vulnerability requires an existing account with the edit_products permission and does not permit data modification, making exploitation dependent on internal access. Business risk is limited to potential exposure of internal software repository structure and content metadata to unauthorized internal users.

Technical Analysis

CVE-2026-12515 is a missing authorization vulnerability (CWE-862) in Katello's content upload functionality within Red Hat Satellite. An authenticated user holding the edit_products permission can query repository content information beyond their authorized scope by exploiting insufficient authorization checks during content upload operations. This constitutes horizontal privilege escalation limited to read access; unauthorized write, import, or publish operations are not affected by this vulnerability. CVSS base score is 4.3 (Medium). The vulnerability maps to MITRE ATT&CK T1078 (Valid Accounts) and T1087 (Account Discovery), reflecting abuse of legitimate credentials to access out-of-scope resources. The authoritative advisory is published at the Red Hat Customer Portal (https://access.redhat.com/security/cve/CVE-2026-12515) and GitHub advisory GHSA-c43c-rf7g-5xpg. Specific affected version ranges should be confirmed from the Red Hat Customer Portal advisory. Patch status should be verified directly against the Red Hat Customer Portal advisory.

Action Checklist

1. Step 1: Containment, Identify all accounts in Red Hat Satellite holding the edit_products permission. Audit whether any of those accounts have accessed repository content outside their intended scope. Consider temporarily restricting edit_products grants to the minimum required users until the patch is applied. Reference: Red Hat Customer Portal advisory for CVE-2026-12515 (https://access.redhat.com/security/cve/CVE-2026-12515). Control: NIST AC-6 (Least Privilege).
2. Step 2: Detection, Query Satellite and Katello application logs for content upload API calls made by accounts with edit_products permission that reference repository IDs outside those accounts' assigned organizations or lifecycle environments. Look for anomalous cross-scope repository query patterns in Foreman audit logs (typically at /var/log/foreman/production.log and /var/log/foreman-proxy/). No IOCs have been published; focus on access pattern anomalies. Control: NIST AU-6 (Audit Record Review, Analysis, and Reporting); CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Apply the vendor-issued patch as documented in the Red Hat Customer Portal advisory for CVE-2026-12515. Confirm the specific patched package version from the advisory before deploying. After patching, re-audit edit_products permission assignments and remove grants not meeting least-privilege requirements. Control: NIST AC-6 (Least Privilege); CIS 7.3 (Perform Automated Operating System Patch Management); CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patching, verify Katello content upload authorization is enforcing scope boundaries by testing with a limited-permission account attempting cross-scope repository queries. Confirm Satellite audit logs are capturing permission-check events for content API calls per NIST AU-12 (Audit Record Generation). Monitor edit_products account activity for 30 days post-patch for anomalous cross-scope access attempts. Control: NIST AU-6; D3FEND D3-UAP (User Account Permissions).
5. Step 5: Post-Incident, Review the authorization model for all Katello permission roles, not only edit_products, to identify similar missing-check patterns. Document findings against NIST AC-3 (Access Enforcement) and AC-5 (Separation of Duties) control gaps. Update access review procedures to include periodic validation that Satellite permission grants align with assigned organizational and lifecycle environment scope. Control: NIST AC-3; NIST AC-5; CIS 6.1 (Establish an Access Granting Process).

Detection Guidance

There are no published IOCs for CVE-2026-12515. Detection relies on log-based access pattern analysis. Review Foreman application logs (/var/log/foreman/production.log) for API calls to Katello content upload endpoints made by accounts holding edit_products permission. Specifically, look for requests that reference repository IDs or organization IDs not associated with the querying account's assigned scope. Foreman audit records (accessible via the Satellite UI under Audit > Audits or via the Foreman API) log permission-relevant actions and should be queried for cross-scope repository reads by limited-permission accounts. Baseline normal repository access patterns per user to distinguish anomalous out-of-scope queries. Align log collection and review with NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting), and CIS 8.2 (Collect Audit Logs). D3FEND countermeasure D3-LAM (Local Account Monitoring) applies: monitor local and application-level account activity for access patterns inconsistent with assigned permissions.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1087** — Account Discovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1087	Account Discovery	Discovery

Sources

Source	URL	Tier
CVE-2026-12515 - Red Hat Customer Portal	https://access.redhat.com/security/cve/CVE-2026-12515	T3
CVE-2026-11015 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-11015	T1
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Source	URL	Tier
A flaw was found in Katello's of Red Hat Satellite. A... · CVE ... - GitHub	https://github.com/advisories/GHSA-c43c-rf7g-5xpg	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-12515	T1

Generated 2026-06-18 17:21 UTC by TJS Security Command Center