



CVE-2017-2662

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-2662
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-22 16:29:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	A flaw was found in Foreman's katello plugin version 3.4.5. After setting a new role to allow restricted access on a repository

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theforeman	Katello	3.4.5	All	All	All
Application	Theforeman	Katello	3.4.5	All	All	All

References

Reference	Source
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
1434106 – (CVE-2017-2662) CVE-2017-2662 foreman: Managing repositories with their id via hammer does not respect the role filters	CONFIRMED
Bug #18838: Managing repositories with their id via hammer does not respect the role filters - Katello - Foreman	CONFIRMED
1434106 – (CVE-2017-2662) CVE-2017-2662 foreman: Managing repositories with their id via hammer does not respect the role filters	MISC
CVE-2017-2662 - Red Hat Customer Portal	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[239228](#) Red Hat Update for Satellite 6.9 (RHSA-2021:1313)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)