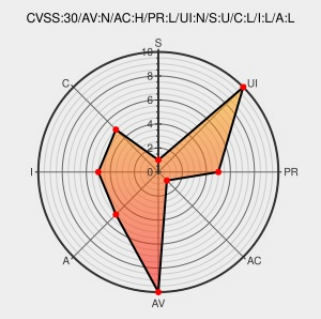
CVE-2016-4451

Published on: 08/19/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:21:00 PM UTC

CVE-2016-4451

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Foreman from Theforeman contain the following vulnerability:

The (1) Organization and (2) Locations APIs in Foreman before 1.11.3 and 1.12.x before 1.12.0-RC1 allow remote authenticated users with unlimited filters to bypass organization and location restrictions and read or modify data for an arbitrary organization by leveraging knowledge of the id of that organization.

CVE-2016-4451 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	LOW

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
1339889 – (CVE-2016-4451) CVE-2016-4451	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1339889

2016-4451 foreman: privilege escalation through Organization and Locations API		
Foreman :: Security	Vendor Advisory theforeman.org text/html	CONFIRM theforeman.org/security.html#2016-4451
CVE-2016-4451 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-4451
Revision 1144040f - Fixes #15182 - limit user taxonomies in API (CVE-2016-4451) - Foreman	Patch Vendor Advisory projects.theforeman.org text/html	CONFIRM projects.theforeman.org/projects/foreman/repository/revisions/1144040f444b4bf4aae81940a150b26b2
Bug #15182: CVE-2016-4451 - Privileges escalation through Organization and Locations API - Foreman	Vendor Advisory projects.theforeman.org text/html	CONFIRM projects.theforeman.org/issues/15182
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:0336

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theforeman	Foreman	1.12.0	All	All	All
Application	Theforeman	Foreman	1.12.0	All	All	All
Application	Theforeman	Foreman	All	All	All	All

cpe:2.3:a:theforeman:foreman:1.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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