



CVE-2016-4995

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

Last Modified on: 02/12/2023 11:22:00 PM UTC

CVE-2016-4995

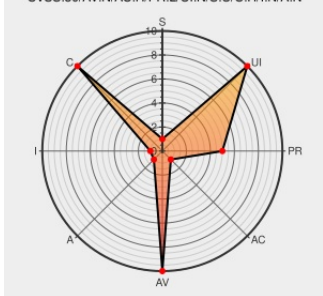
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Foreman](#) from [Theforeman](#) contain the following vulnerability:

Foreman before 1.11.4 and 1.12.x before 1.12.1 does not properly restrict access to preview provisioning templates, which allows remote authenticated users with permission to view some hosts to obtain sensitive host configuration information via a URL with a hostname.

CVE-2016-4995 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Revision c3c186de - Fixes #15490 - adding view_host filter and better msg	Patch Vendor Advisory projects.theforeman.org text/html	CONFIRM projects.theforeman.org/projects/foreman/repository/revisions/c3c186de12be15e55d9582e5465/

Users who are
logged i... -
Foreman

1348939 – (CVE-2016-4995) CVE-2016-4995
foreman:
Information
disclosure in
provisioning
template
previews

[bugzilla.redhat.com](#)
[text/html](#)

 [MISC bugzilla.redhat.com/show_bug.cgi?id=1348939](#)

CVE-2016-4995 -
Red Hat
Customer Portal

[access.redhat.com](#)
[text/html](#)

 [MISC access.redhat.com/security/cve/CVE-2016-4995](#)

Red Hat
Customer Portal

[Third Party Advisory](#)
[access.redhat.com](#)
[text/html](#)

 [REDHAT RHSA-2018:0336](#)

Foreman ::
Security

[Vendor Advisory](#)
[theforeman.org](#)
[text/html](#)

 [CONFIRM theforeman.org/security.html#2016-4995](#)

Bug #15490:
CVE-2016-4995 -
view_hosts
permissions/filters
not checked for
provisioning
template
previews -
Foreman

[Patch](#)
[Vendor Advisory](#)
[projects.theforeman.org](#)
[text/html](#)

 [CONFIRM projects.theforeman.org/issues/15490](#)

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	All	All	All	All
Application	Theforeman	Foreman	All	All	All	All

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

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 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](#)