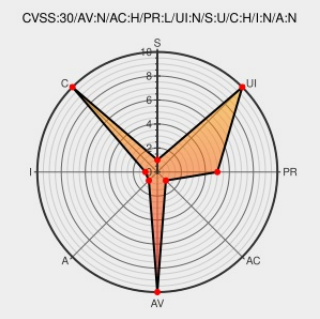
CVE-2016-4995

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



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

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 and Source URL Uptime Status status.cve.report