



CVE-2014-3691

Published on: 03/09/2015 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:42:00 AM UTC

CVE-2014-3691

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Openstack](#) from [Redhat](#) contain the following vulnerability:

Smart Proxy (aka Smart-Proxy and foreman-proxy) in Foreman before 1.5.4 and 1.6.x before 1.6.2 does not validate SSL certificates, which allows remote attackers to bypass intended authentication and execute arbitrary API requests via a request without a certificate.

CVE-2014-3691 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Red Hat Customer Portal

[access.redhat.com](https://access.redhat.com/text/html)
text/html

MISC access.redhat.com/errata/RHSA-2015:0287

Google Groups

[groups.google.com](https://groups.google.com/text/html)
text/html

MISC groups.google.com/forum/#%21topic/foreman-announce/jXC5ixybjqo

Red Hat Customer Portal

Third Party Advisory
[web.archive.org](https://web.archive.org/text/html)
text/html
Inactive Link Not Archived

REDHAT RHSA-2015:0288

1150879 – (CVE-2014-3691) CVE-2014-3691 foreman-proxy: failure to verify SSL certificates

[bugzilla.redhat.com](https://bugzilla.redhat.com/text/html)
text/html

MISC bugzilla.redhat.com/show_bug.cgi?id=1150879

Bug #7822: CVE-2014-3691 - Smart proxy doesn't perform verification of client SSL certificate on API requests - Smart-

Vendor Advisory
projects.theforeman.org

CONFIRM projects.theforeman.org/issues/7822

Proxy - Foreman	text/html	
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:0287
fixes #7822 - forbid HTTPS requests with no client SSL certificate by domcleal · Pull Request #217 · theforeman/smart-proxy · GitHub	Issue Tracking Patch github.com text/html	 CONFIRM github.com/theforeman/smart-proxy/pull/217
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2015:0288
access.redhat.com CVE-2014-3691	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2014-3691
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHBA-2015:0054

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	Redhat	Openstack	4.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	4.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Theforeman	Foreman	1.6.0	All	All	All
Application	Theforeman	Foreman	1.6.1	All	All	All
Application	Theforeman	Foreman	1.6.0	All	All	All
Application	Theforeman	Foreman	1.6.1	All	All	All
Application	Theforeman	Foreman	All	All	All	All
cpe:2.3:a:redhat:openstack:4.0:*****:*.:						
cpe:2.3:a:redhat:openstack:5.0:*****:*.:						
cpe:2.3:a:redhat:openstack:4.0:*****:*.:						
cpe:2.3:a:redhat:openstack:5.0:*****:*.:						
cpe:2.3:a:theforeman:foreman:1.6.0:*****:*.:						
cpe:2.3:a:theforeman:foreman:1.6.1:*****:*.:						

cpe:2.3:a:theforeman:foreman:1.6.0:*:*:*:*:*:
cpe:2.3:a:theforeman:foreman:1.6.1:*:*:*:*:*:
cpe:2.3:a:theforeman:foreman:*:*:*:*:*:

```
cpe:2.3:a:theforeman:foreman:1.6.1:*:*:*:*:*:
```

```
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