

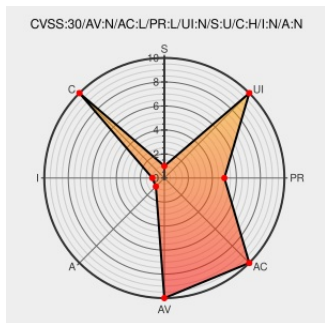


CVE-2014-3250

Published on: 12/11/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3250

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

The default vhost configuration file in Puppet before 3.6.2 does not include the SSLCARevocationCheck directive, which might allow remote attackers to obtain sensitive information via a revoked certificate when a Puppet master runs with Apache 2.4.

CVE-2014-3250 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
CVE-2014-3250 Puppet	Vendor Advisory puppet.com text/html	CONFIRM puppet.com/security/cve/CVE-2014-3250
1101347 – (CVE-2014-3250) CVE-2014-3250 puppet: certificates could be	Issue Tracking	CONFIRM

Patch bugzilla.redhat.com/show_bug.cgi?id=1101347

Third Party Advisory

bugzilla.redhat.com

[text/html](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.0	All	All	All
Application	Apache	Http Server	2.4.0	All	All	All
Application	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet	All	All	All	All
Operating System	Redhat	Linux	-	All	All	All
Operating System	Redhat	Linux	-	All	All	All
cpe:2.3:a:apache:http_server:2.4.0:*****:*.:						
cpe:2.3:a:apache:http_server:2.4.0:*****:*.:						
cpe:2.3:a:puppet:puppet:*****:*.:						
cpe:2.3:a:puppet:puppet:*****:*.:						
cpe:2.3:o:redhat:linux:-:*****:*.:						
cpe:2.3:o:redhat:linux:-:*****:*.:						

[← Previous ID](#)

Next ID→

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.report and Source URL Uptime Status status.cve.report