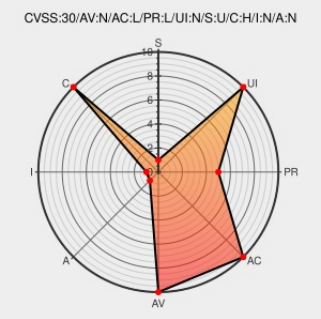
# CVE-2014-3250

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 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<br>puppet.com<br>text/html | CONFIRM<br>puppet.com/security/cve/CVE-2014-3250 |
| 1101347 – (CVE-2014-3250) CVE-2014-3250 puppet: certificates could be | Issue Tracking | CONFIRM |

| | | |
|---|---|---|
| honored even when revoked | Patch<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | bugzilla.redhat.com/show_bug.cgi?id=1101347 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| 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:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→