



CVE-2011-3848

Published on: 10/27/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:14 PM UTC

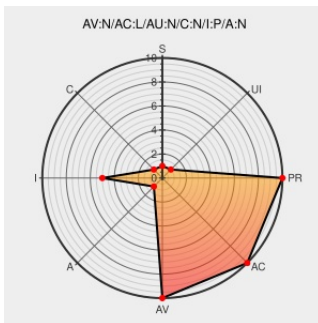
CVE-2011-3848

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Directory traversal vulnerability in Puppet 2.6.x before 2.6.10 and 2.7.x before 2.7.4 allows remote attackers to write X.509 Certificate Signing Request (CSR) to arbitrary locations via (1) a double-encoded key parameter in the URI in 2.7.x, (2) the CN in the Subject of a CSR in 2.6 and 0.25.

CVE-2011-3848 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
openSUSE-SU-2011:1190-1: moderate: puppet (CVE-2011-3848)	lists.opensuse.org text/html	SUSE openSUSE-SU-2011:1190
Security Advisory SA46628 - SUSE update for puppet - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 46628
USN-1217-1: Puppet vulnerability Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1217-1
Debian -- Security Information -- DSA-2314-1 puppet	www.debian.org Deprecated Link text/html	DEBIAN DSA-2314
CVE-2011-3848 Puppet	puppet.com	CONFIRM puppet.com/security/cve/cve-2011-3848

[text/html](#)

Google Groups

[Patch](#)[groups.google.com](#)[text/html](#) [CONFIRM groups.google.com/group/puppet-announce/browse_thread/thread/e57ce2740feb9406](https://groups.google.com/group/puppet-announce/browse_thread/thread/e57ce2740feb9406)

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	Puppet	Puppet	2.6.0	All	All	All
Application	Puppet	Puppet	2.6.1	All	All	All
Application	Puppet	Puppet	2.6.2	All	All	All
Application	Puppet	Puppet	2.6.3	All	All	All
Application	Puppet	Puppet	2.6.4	All	All	All
Application	Puppet	Puppet	2.6.5	All	All	All
Application	Puppet	Puppet	2.6.6	All	All	All
Application	Puppet	Puppet	2.6.7	All	All	All
Application	Puppet	Puppet	2.6.8	All	All	All
Application	Puppet	Puppet	2.6.9	All	All	All
Application	Puppet	Puppet	2.7.2	All	All	All
Application	Puppet	Puppet	2.7.3	All	All	All
Application	Puppet	Puppet	2.6.0	All	All	All
Application	Puppet	Puppet	2.6.1	All	All	All
Application	Puppet	Puppet	2.6.2	All	All	All
Application	Puppet	Puppet	2.6.3	All	All	All
Application	Puppet	Puppet	2.6.4	All	All	All
Application	Puppet	Puppet	2.6.5	All	All	All
Application	Puppet	Puppet	2.6.6	All	All	All
Application	Puppet	Puppet	2.6.7	All	All	All
Application	Puppet	Puppet	2.6.8	All	All	All
Application	Puppet	Puppet	2.6.9	All	All	All
Application	Puppet	Puppet	2.7.2	All	All	All
Application	Puppet	Puppet	2.7.3	All	All	All
Application	Puppetlabs	Puppet	2.7.0	All	All	All

Application	Puppetlabs	Puppet	2.7.1	All	All	All
Application	Puppetlabs	Puppet	2.7.0	All	All	All
Application	Puppetlabs	Puppet	2.7.1	All	All	All
cpe:2.3:a:puppet:puppet:2.6.0:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.1:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.2:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.3:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.4:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.5:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.6:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.7:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.8:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.9:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.7.2:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.7.3:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.0:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.1:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.2:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.3:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.4:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.5:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.6:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.7:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.8:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.6.9:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.7.2:*:*:*:*:*:						
cpe:2.3:a:puppet:puppet:2.7.3:*:*:*:*:*:						
cpe:2.3:a:puppetlabs:puppet:2.7.0:*:*:*:*:*:						
cpe:2.3:a:puppetlabs:puppet:2.7.1:*:*:*:*:*:						

cpe:2.3:a:puppetlabs:puppet:2.7.0:*****:

cpe:2.3:a:puppetlabs:puppet:2.7.1:*****:

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](#)