



CVE-2012-3867

Published on: 08/06/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:17 PM UTC

CVE-2012-3867

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

lib/puppet/ssl/certificate_authority.rb in Puppet before 2.6.17 and 2.7.x before 2.7.18, and Puppet Enterprise before 2.5.2, does not properly restrict the characters in the Common Name field of a Certificate Signing Request (CSR), which makes it easier for user-assisted remote attackers to trick administrators into signing a crafted agent certificate

via ANSI control sequences.

CVE-2012-3867 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Validate CSR CN and provided certname before signing · puppetlabs/puppet@f341962 · GitHub

[Exploit](#)
[Issue Tracking](#)
[Patch](#)
[github.com](#)
[text/html](#)

CONFIRM
github.com/puppetlabs/puppet/commit/f3419620b42080dad3b0be14470b20a972f13c50

CVE-2012-3867 | Puppet Labs

[Vendor Advisory](#)
[puppetlabs.com](#)
[text/html](#)

CONFIRM puppetlabs.com/security/cve/cve-2012-3867/

openSUSE-SU-2012:0891-1: moderate: puppet for multiple issues

[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

SUSE [openSUSE-SU-2012:0891](https://www.suse.com/support/update/updates/view.php?id=118991)

Debian -- Security Information -- DSA-2511-1 puppet	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-2511
USN-1506-1: Puppet vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-1506-1
Security Advisory SA50014 - SUSE update for puppet - Secunia	web.archive.org text/html	 SECUNIA 50014
[security-announce] SUSE-SU-2012:0983-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2012:0983
Validate CSR CN and provided certname before signing · puppetlabs/puppet@dfedaa5 · GitHub	Exploit Issue Tracking Patch github.com text/html	 CONFIRM github.com/puppetlabs/puppet/commit/dfedaa5fa841ccf335245a748b347b7c7c236640
839158 – (CVE-2012-3867) CVE-2012-3867 puppet: insufficient validation of agent names in CN of SSL certificate requests	Issue Tracking bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=839158

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
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Application	Puppet	Puppet	2.6.0	All	All	All
Application	Puppet	Puppet	2.6.1	All	All	All
Application	Puppet	Puppet	2.6.10	All	All	All
Application	Puppet	Puppet	2.6.11	All	All	All
Application	Puppet	Puppet	2.6.12	All	All	All
Application	Puppet	Puppet	2.6.13	All	All	All
Application	Puppet	Puppet	2.6.14	All	All	All
Application	Puppet	Puppet	2.6.15	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	2.7.10	All	All	All
Application	Puppet	Puppet	2.7.11	All	All	All
Application	Puppet	Puppet	2.7.12	All	All	All
Application	Puppet	Puppet	2.7.13	All	All	All
Application	Puppet	Puppet	2.7.14	All	All	All
Application	Puppet	Puppet	2.7.16	All	All	All
Application	Puppet	Puppet	2.7.17	All	All	All
Application	Puppet	Puppet	2.7.2	All	All	All
Application	Puppet	Puppet	2.7.3	All	All	All
Application	Puppet	Puppet	2.7.4	All	All	All

Application	Puppet	Puppet	2.7.5	All	All	All
Application	Puppet	Puppet	2.7.6	All	All	All
Application	Puppet	Puppet	2.7.7	All	All	All
Application	Puppet	Puppet	2.7.8	All	All	All
Application	Puppet	Puppet	2.7.9	All	All	All
Application	Puppet	Puppet	2.6.0	All	All	All
Application	Puppet	Puppet	2.6.1	All	All	All
Application	Puppet	Puppet	2.6.10	All	All	All
Application	Puppet	Puppet	2.6.11	All	All	All
Application	Puppet	Puppet	2.6.12	All	All	All
Application	Puppet	Puppet	2.6.13	All	All	All
Application	Puppet	Puppet	2.6.14	All	All	All
Application	Puppet	Puppet	2.6.15	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	2.7.10	All	All	All
Application	Puppet	Puppet	2.7.11	All	All	All
Application	Puppet	Puppet	2.7.12	All	All	All
Application	Puppet	Puppet	2.7.13	All	All	All
Application	Puppet	Puppet	2.7.14	All	All	All
Application	Puppet	Puppet	2.7.16	All	All	All
Application	Puppet	Puppet	2.7.17	All	All	All
Application	Puppet	Puppet	2.7.2	All	All	All
Application	Puppet	Puppet	2.7.3	All	All	All
Application	Puppet	Puppet	2.7.4	All	All	All
Application	Puppet	Puppet	2.7.5	All	All	All
Application	Puppet	Puppet	2.7.6	All	All	All
Application	Puppet	Puppet	2.7.7	All	All	All
Application	Puppet	Puppet	2.7.8	All	All	All

cpe:2.3:o:opensuse:opensuse:11.4:~::~~::~~::
cpe:2.3:o:opensuse:opensuse:12.1:~::~~::~~::
cpe:2.3:o:opensuse:opensuse:11.4:~::~~::~~::
cpe:2.3:o:opensuse:opensuse:12.1:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.0:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.1:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.10:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.11:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.12:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.13:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.14:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.6.15:~::~~::~~::
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:2.7.10:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.11:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.12:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.13:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.14:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.16:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.17:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.2:~::~~::~~::
cpe:2.3:a:puppet:puppet:2.7.3:~::~~::~~::

cpe:2.3:a:puppet:puppet:2.7.4:*****:
cpe:2.3:a:puppet:puppet:2.7.5:*****:
cpe:2.3:a:puppet:puppet:2.7.6:*****:
cpe:2.3:a:puppet:puppet:2.7.7:*****:
cpe:2.3:a:puppet:puppet:2.7.8:*****:
cpe:2.3:a:puppet:puppet:2.7.9:*****:
cpe:2.3:a:puppet:puppet:2.6.0:*****:
cpe:2.3:a:puppet:puppet:2.6.1:*****:
cpe:2.3:a:puppet:puppet:2.6.10:*****:
cpe:2.3:a:puppet:puppet:2.6.11:*****:
cpe:2.3:a:puppet:puppet:2.6.12:*****:
cpe:2.3:a:puppet:puppet:2.6.13:*****:
cpe:2.3:a:puppet:puppet:2.6.14:*****:
cpe:2.3:a:puppet:puppet:2.6.15:*****:
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:2.7.10:*****:
cpe:2.3:a:puppet:puppet:2.7.11:*****:
cpe:2.3:a:puppet:puppet:2.7.12:*****:
cpe:2.3:a:puppet:puppet:2.7.13:*****:
cpe:2.3:a:puppet:puppet:2.7.14:*****:
cpe:2.3:a:puppet:puppet:2.7.16:*****:

```
cpe:2.3:a:puppet:puppet:2.7.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet:2.7.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:*:*:*:*:*:*:
```

```
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:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppetlabs:puppet:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*.:.:.:.:
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:*:*:
```

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](#)