



# CVE-2016-5714

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-5714
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-18 18:29:00 UTC
<b>Updated</b>	2022-01-24 16:46:00 UTC
<b>Description</b>	Puppet Enterprise 2015.3.3 and 2016.x before 2016.4.0, and Puppet Agent 1.3.6 through 1.7.0 allow remote attackers to by

## Risk And Classification

**Problem Types:** CWE-284

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Puppet</a>	<a href="#">Puppet</a>	2015.3.3	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet</a>	2016.1.1	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet</a>	2016.1.2	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet</a>	2016.2.0	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet</a>	2016.2.1	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Agent</a>	All	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2015.3.3	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.1.1	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.1.2	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.2.0	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.2.1	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2015.3.3	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.1.1	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.1.2	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.2.0	All	All	All
Application	<a href="#">Puppet</a>	<a href="#">Puppet Enterprise</a>	2016.2.1	All	All	All
Application	<a href="#">Puppetlabs</a>	<a href="#">Puppet Agent</a>	1.3.6	All	All	All

Application	Puppetlabs	Puppet Agent	1.4.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.4.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.4.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.3	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.7.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.3.6	All	All	All
Application	Puppetlabs	Puppet Agent	1.4.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.4.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.4.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.5.3	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.0	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.1	All	All	All
Application	Puppetlabs	Puppet Agent	1.6.2	All	All	All
Application	Puppetlabs	Puppet Agent	1.7.0	All	All	All

## References

### Reference

[Puppet Agent: Multiple vulnerabilities \(GLSA 201710-12\) — Gentoo security](#)

[CVE-2016-5714 - Unprivileged Access to Environment Catalogs | Puppet](#)

[597684 – \(CVE-2016-5714\) <app-admin/puppet-agent-1.7.1: Puppet Execution Protocol \(PXP\) Command Whitelist Validation Vulnerability](#)

[Puppet Execution Protocol \(PXP\) Command Whitelist Validation Vulnerability | Puppet](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

710410 Gentoo Linux Puppet Agent Multiple Vulnerabilities (GLSA 201710-12)

© [CVE.report](#) 2026 |

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](#)**