



CVE-2017-10689

Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

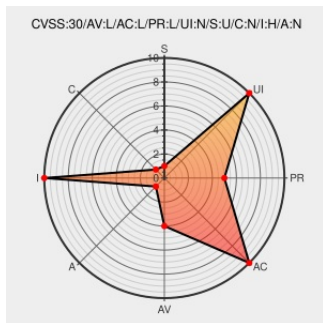
CVE-2017-10689

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In previous versions of Puppet Agent it was possible to install a module with world writable permissions. Puppet Agent 5.3.4 and 1.10.10 included a fix to this vulnerability.

CVE-2017-10689 has been assigned by security@puppet.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Puppet - Puppet Enterprise** version **prior to 2016.4.10 or 2017.3.4**

Affected Vendor/Software: **Puppet - Puppet Agent** version **prior to 5.3.4 or 1.10.10**

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
CVE-2017-10689: A vulnerability in the Puppet Agent software allows an attacker to install a module with world writable permissions. This vulnerability is present in versions of Puppet Agent prior to 5.3.4 and 1.10.10.	CONFIRMED	Puppet Security Advisories

CVE-2017-10689 - Insecure permissions on some modules when installing with PE Puppet	Vendor Advisory puppet.com text/html	CONFIRM puppet.com/security/cve/CVE-2017-10689
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2927
USN-3567-1: Puppet vulnerability Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3567-1

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Application	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All
Application	Redhat	Satellite	6.4	All	All	All
Application	Redhat	Satellite	6.4	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:*:*:

cpe:2.3:a:puppet:puppet:*:*:*:*:*:

cpe:2.3:a:puppet:puppet:*:*:*:*:*:

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

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

cpe:2.3:a:redhat:satellite:6.4:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:6.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [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](#)