



# CVE-2017-9232

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

## Summary

<b>CVE</b>	CVE-2017-9232
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-28 00:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	Juju before 1.25.12, 2.0.x before 2.0.4, and 2.1.x before 2.1.3 uses a UNIX domain socket without setting appropriate perm

## Risk And Classification

**Problem Types:** CWE-862

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	All	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	alpha1	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	alpha2	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta1	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta10	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta11	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta12	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta13	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta14	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta15	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta16	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta17	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta18	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta2	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta3	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta4	All	All
Application	<a href="#">Canonical</a>	<a href="#">Juju</a>	2.0.0	beta5	All	All

Application	Canonical	Juju	2.0.0	beta6	All	All
Application	Canonical	Juju	2.0.0	beta7	All	All
Application	Canonical	Juju	2.0.0	beta8	All	All
Application	Canonical	Juju	2.0.0	beta9	All	All
Application	Canonical	Juju	2.0.0	rc1	All	All
Application	Canonical	Juju	2.0.0	rc2	All	All
Application	Canonical	Juju	2.0.0	rc3	All	All
Application	Canonical	Juju	2.0.1	All	All	All
Application	Canonical	Juju	2.0.2	All	All	All
Application	Canonical	Juju	2.0.3	All	All	All
Application	Canonical	Juju	2.1.0	All	All	All
Application	Canonical	Juju	2.1.0	beta1	All	All
Application	Canonical	Juju	2.1.0	beta2	All	All
Application	Canonical	Juju	2.1.0	beta3	All	All
Application	Canonical	Juju	2.1.0	beta4	All	All
Application	Canonical	Juju	2.1.0	beta5	All	All
Application	Canonical	Juju	2.1.0	rc1	All	All
Application	Canonical	Juju	2.1.0	rc2	All	All
Application	Canonical	Juju	2.1.1	All	All	All
Application	Canonical	Juju	2.1.2	All	All	All
Application	Canonical	Juju	2.0.0	All	All	All
Application	Canonical	Juju	2.0.0	alpha1	All	All
Application	Canonical	Juju	2.0.0	alpha2	All	All
Application	Canonical	Juju	2.0.0	beta1	All	All
Application	Canonical	Juju	2.0.0	beta10	All	All
Application	Canonical	Juju	2.0.0	beta11	All	All
Application	Canonical	Juju	2.0.0	beta12	All	All
Application	Canonical	Juju	2.0.0	beta13	All	All
Application	Canonical	Juju	2.0.0	beta14	All	All
Application	Canonical	Juju	2.0.0	beta15	All	All
Application	Canonical	Juju	2.0.0	beta16	All	All
Application	Canonical	Juju	2.0.0	beta17	All	All
Application	Canonical	Juju	2.0.0	beta18	All	All
Application	Canonical	Juju	2.0.0	beta2	All	All
Application	Canonical	Juju	2.0.0	beta3	All	All

Application	Canonical	Juju	2.0.0	beta4	All	All
Application	Canonical	Juju	2.0.0	beta5	All	All
Application	Canonical	Juju	2.0.0	beta6	All	All
Application	Canonical	Juju	2.0.0	beta7	All	All
Application	Canonical	Juju	2.0.0	beta8	All	All
Application	Canonical	Juju	2.0.0	beta9	All	All
Application	Canonical	Juju	2.0.0	rc1	All	All
Application	Canonical	Juju	2.0.0	rc2	All	All
Application	Canonical	Juju	2.0.0	rc3	All	All
Application	Canonical	Juju	2.0.1	All	All	All
Application	Canonical	Juju	2.0.2	All	All	All
Application	Canonical	Juju	2.0.3	All	All	All
Application	Canonical	Juju	2.1.0	All	All	All
Application	Canonical	Juju	2.1.0	beta1	All	All
Application	Canonical	Juju	2.1.0	beta2	All	All
Application	Canonical	Juju	2.1.0	beta3	All	All
Application	Canonical	Juju	2.1.0	beta4	All	All
Application	Canonical	Juju	2.1.0	beta5	All	All
Application	Canonical	Juju	2.1.0	rc1	All	All
Application	Canonical	Juju	2.1.0	rc2	All	All
Application	Canonical	Juju	2.1.1	All	All	All
Application	Canonical	Juju	2.1.2	All	All	All
Application	Canonical	Juju	All	All	All	All

## References

Reference	Source	Link	Tags
Bug #1682411 "juju-run unit root escalation vulnerability" : Bugs : juju	CONFIRM	<a href="https://bugs.launchpad.net">bugs.launchpad.net</a>	Exploit, Issue Tracking, This
Juju-run Agent - Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	
Juju CVE-2017-8849 Local Privilege Escalation Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB E
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

---

© [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](#)**