

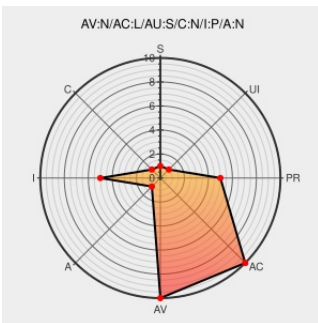


CVE-2013-1901

Published on: 04/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:33 PM UTC

CVE-2013-1901

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

PostgreSQL 9.2.x before 9.2.4 and 9.1.x before 9.1.9 does not properly check REPLICATION privileges, which allows remote authenticated users to bypass intended backup restrictions by calling the (1) `pg_start_backup` or (2) `pg_stop_backup` functions.

CVE-2013-1901 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

About the security content of OS X Server v2.2.2

[support.apple.com
text/html](https://support.apple.com/text/html)

[CONFIRM support.apple.com/kb/HT5892](https://support.apple.com/kb/HT5892)

[security-announce] openSUSE-SU-2013:0627-1: important: postgresql91 to

[lists.opensuse.org
text/html](https://lists.opensuse.org/text/html)

[SUSE openSUSE-SU-2013:0627](https://www.suse.com/openSUSE-SU-2013:0627)

APPLE-SA-2013-09-17-1 OS X Server v2.2.2

[lists.apple.com
text/html](https://lists.apple.com/text/html)

[APPLE APPLE-SA-2013-09-17-1](https://support.apple.com/kb/HT5892)

APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004

[lists.apple.com
text/html](https://lists.apple.com/text/html)

[APPLE APPLE-SA-2013-09-12-1](https://support.apple.com/kb/HT5892)

[SECURITY] Fedora 19 Update: postgresql-9.2.4-1.fc19

[lists.fedoraproject.org
text/html](https://lists.fedoraproject.org/text/html)

[FEDORA FEDORA-2013-6148](https://www.fedoraproject.org/FEDORA-2013-6148)

PostgreSQL: Documentation: 9.3: Release 9.2.4

[web.archive.org
text/html](https://web.archive.org/text/html)

[CONFIRM
www.postgresql.org/docs/current/static/release-](https://www.postgresql.org/docs/current/static/release-9.2.4.html)

Inactive Link Not Archived 9-2-4.html

PostgreSQL: Documentation: 9.3: Release 9.1.9

www.postgresql.org
text/html

CONFIRM
www.postgresql.org/docs/current/static/release-9-1-9.html

About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

support.apple.com
text/html

CONFIRM support.apple.com/kb/HT5880

USN-1789-1: PostgreSQL vulnerabilities | Ubuntu

www.ubuntu.com
text/html

UBUNTU USN-1789-1

[security-announce] openSUSE-SU-2013:0628-1: important: postgresql92: Va

lists.opensuse.org
text/html

SUSE openSUSE-SU-2013:0628

[security-announce] openSUSE-SU-2013:0635-1: important: postgresql: secu

lists.opensuse.org
text/html

SUSE openSUSE-SU-2013:0635

PostgreSQL: PostgreSQL 9.2.4, 9.1.9, 9.0.13 and 8.4.17 released

Vendor Advisory
www.postgresql.org
text/html

CONFIRM
www.postgresql.org/about/news/1456/

Support / Security / Advisories // MDVSA-2013:142 | Mandriva

www.mandriva.com
text/html

MANDRIVA MDVSA-2013:142

Debian -- Security Information -- DSA-2658-1 postgresql-9.1

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-2658

[SECURITY] Fedora 17 Update: postgresql-9.1.9-1.fc17

lists.fedoraproject.org
text/html

FEDORA FEDORA-2013-5000

[security-announce] SUSE-SU-2013:0633-1: important: Security update for

lists.opensuse.org
text/html

SUSE SUSE-SU-2013:0633

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	-	Its	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All

Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	-	lts	All
Application	Postgresql	Postgresql	9.1	All	All	All
Application	Postgresql	Postgresql	9.1.1	All	All	All
Application	Postgresql	Postgresql	9.1.2	All	All	All
Application	Postgresql	Postgresql	9.1.3	All	All	All
Application	Postgresql	Postgresql	9.1.4	All	All	All
Application	Postgresql	Postgresql	9.1.5	All	All	All
Application	Postgresql	Postgresql	9.1.6	All	All	All
Application	Postgresql	Postgresql	9.1.7	All	All	All
Application	Postgresql	Postgresql	9.1.8	All	All	All
Application	Postgresql	Postgresql	9.2	All	All	All
Application	Postgresql	Postgresql	9.2.1	All	All	All
Application	Postgresql	Postgresql	9.2.2	All	All	All
Application	Postgresql	Postgresql	9.2.3	All	All	All
Application	Postgresql	Postgresql	9.1	All	All	All
Application	Postgresql	Postgresql	9.1.1	All	All	All
Application	Postgresql	Postgresql	9.1.2	All	All	All
Application	Postgresql	Postgresql	9.1.3	All	All	All
Application	Postgresql	Postgresql	9.1.4	All	All	All
Application	Postgresql	Postgresql	9.1.5	All	All	All
Application	Postgresql	Postgresql	9.1.6	All	All	All
Application	Postgresql	Postgresql	9.1.7	All	All	All
Application	Postgresql	Postgresql	9.1.8	All	All	All
Application	Postgresql	Postgresql	9.2	All	All	All
Application	Postgresql	Postgresql	9.2.1	All	All	All
Application	Postgresql	Postgresql	9.2.2	All	All	All
Application	Postgresql	Postgresql	9.2.3	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:8.04:-:lts:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:8.04:-:lts:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.2:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.3:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.4:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.5:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.6:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.7:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.8:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.2:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.2.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.2.2:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.2.3:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.2:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.3:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.4:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.5:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.6:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:9.1.7:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql:9.1.8:*****:	
cpe:2.3:a:postgresql:postgresql:9.2:*****:	
cpe:2.3:a:postgresql:postgresql:9.2.1:*****:	
cpe:2.3:a:postgresql:postgresql:9.2.2:*****:	
cpe:2.3:a:postgresql:postgresql:9.2.3:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→