

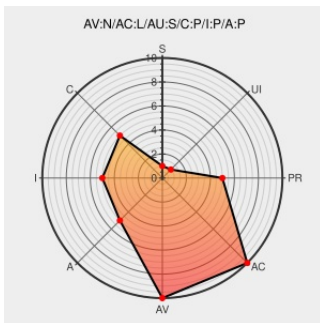


CVE-2013-1899

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

Last Modified on: 03/23/2021 11:28:32 PM UTC

CVE-2013-1899

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

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

Argument injection vulnerability in PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, and 9.0.x before 9.0.13 allows remote attackers to cause a denial of service (file corruption), and allows remote authenticated users to modify configuration settings and execute arbitrary code, via a connection request using a database name that begins with a "-"

(hyphen).

CVE-2013-1899 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
About the security content of OS X Server v2.2.2	support.apple.com text/html	CONFIRM support.apple.com/kb/HT5892
PostgreSQL: Documentation: 9.3: Release 9.0.13	www.postgresql.org text/html	CONFIRM www.postgresql.org/docs/current/static/release-9-0-13.html
[security-announce] openSUSE-SU-2013:0627-1: important: postgresql91 to	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0627
APPLE-SA-2013-09-17-1 OS X Server v2.2.2	lists.apple.com text/html	APPLE APPLE-SA-2013-09-17-1
APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and	lists.apple.com	APPLE APPLE-SA-2013-09-12-1

Security Update 2013-004	text/html	
[SECURITY] Fedora 19 Update: postgresql-9.2.4-1.fc19	lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-6148
PostgreSQL: Documentation: 9.3: Release 9.2.4	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.postgresql.org/docs/current/static/release-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/
PostgreSQL: 2013-04-04 Security Release FAQ	Vendor Advisory www.postgresql.org text/html	 CONFIRM www.postgresql.org/support/security/faq/2013-04-04/
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	Canonical	Ubuntu Linux	12.04	-	Its	All

System						
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	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	-	Its	All
Application	Postgresql	Postgresql	9.0	All	All	All
Application	Postgresql	Postgresql	9.0.1	All	All	All
Application	Postgresql	Postgresql	9.0.10	All	All	All
Application	Postgresql	Postgresql	9.0.11	All	All	All
Application	Postgresql	Postgresql	9.0.12	All	All	All
Application	Postgresql	Postgresql	9.0.2	All	All	All
Application	Postgresql	Postgresql	9.0.3	All	All	All
Application	Postgresql	Postgresql	9.0.4	All	All	All
Application	Postgresql	Postgresql	9.0.5	All	All	All
Application	Postgresql	Postgresql	9.0.6	All	All	All
Application	Postgresql	Postgresql	9.0.7	All	All	All
Application	Postgresql	Postgresql	9.0.8	All	All	All
Application	Postgresql	Postgresql	9.0.9	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
Application	Postgresql	Postgresql	9.0	All	All	All
Application	Postgresql	Postgresql	9.0.1	All	All	All
Application	Postgresql	Postgresql	9.0.10	All	All	All
Application	Postgresql	Postgresql	9.0.11	All	All	All
Application	Postgresql	Postgresql	9.0.12	All	All	All
Application	Postgresql	Postgresql	9.0.2	All	All	All
Application	Postgresql	Postgresql	9.0.3	All	All	All
Application	Postgresql	Postgresql	9.0.4	All	All	All
Application	Postgresql	Postgresql	9.0.5	All	All	All
Application	Postgresql	Postgresql	9.0.6	All	All	All
Application	Postgresql	Postgresql	9.0.7	All	All	All
Application	Postgresql	Postgresql	9.0.8	All	All	All
Application	Postgresql	Postgresql	9.0.9	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:9.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.1:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:postgresql:postgresql:9.0.10:*:*:*:*:*:*:*
```

```
cpe:2.3:a:postgresql:postgresql:9.0.11:::*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.12:*:*:*:*:*:*:*
```

```
cpe:2.3:a:postgresql:postgresql:9.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.5:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.7:*:*:*:*:*:*.*
```

```
cpe:2.3:a:postgresql:postgresql:9.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:postgresql:postgresql:9.0.9:*:*:*:*:*:*:
```

```
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:9.0:*****:
cpe:2.3:a:postgresql:postgresql:9.0.1:*****:
cpe:2.3:a:postgresql:postgresql:9.0.10:*****:
cpe:2.3:a:postgresql:postgresql:9.0.11:*****:
cpe:2.3:a:postgresql:postgresql:9.0.12:*****:
cpe:2.3:a:postgresql:postgresql:9.0.2:*****:
cpe:2.3:a:postgresql:postgresql:9.0.3:*****:
cpe:2.3:a:postgresql:postgresql:9.0.4:*****:
cpe:2.3:a:postgresql:postgresql:9.0.5:*****:
cpe:2.3:a:postgresql:postgresql:9.0.6:*****:
cpe:2.3:a:postgresql:postgresql:9.0.7:*****:
cpe:2.3:a:postgresql:postgresql:9.0.8:*****:
cpe:2.3:a:postgresql:postgresql:9.0.9:*****:
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→

© [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](#)