

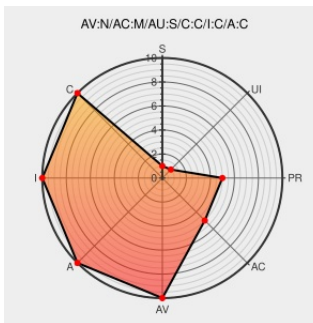


CVE-2013-1900

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

Last Modified on: 03/23/2021 11:28:31 PM UTC

CVE-2013-1900

[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, 9.1.x before 9.1.9, 9.0.x before 9.0.13, and 8.4.x before 8.4.17, when using OpenSSL, generates insufficiently random numbers, which might allow remote authenticated users to have an unspecified impact via vectors related to the "contrib/pgcrypto functions."

CVE-2013-1900 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
PostgreSQL: Documentation: 9.3: Release 8.4.17	www.postgresql.org text/html	CONFIRM www.postgresql.org/docs/current/static/release-8-4-17.html
About the security content of OS X Server v2.2.2	support.apple.com text/html	CONFIRM support.apple.com/kb/HT5892
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1475
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-2013:062/-1: important: postgresql91 to	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:062/
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 Security Update 2013-004	lists.apple.com text/html	 APPLE APPLE-SA-2013-09-12-1
[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/
Debian -- Security Information -- DSA-2657-1 postgresql-8.4	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2657
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
Oracle Critical Patch Update - October 2017	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
[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)

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	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	8.4	All	All	All
Application	Postgresql	Postgresql	8.4.1	All	All	All
Application	Postgresql	Postgresql	8.4.10	All	All	All
Application	Postgresql	Postgresql	8.4.11	All	All	All
Application	Postgresql	Postgresql	8.4.12	All	All	All
Application	Postgresql	Postgresql	8.4.13	All	All	All
Application	Postgresql	Postgresql	8.4.14	All	All	All
Application	Postgresql	Postgresql	8.4.15	All	All	All
Application	Postgresql	Postgresql	8.4.16	All	All	All
Application	Postgresql	Postgresql	8.4.2	All	All	All
Application	Postgresql	Postgresql	8.4.3	All	All	All
Application	Postgresql	Postgresql	8.4.4	All	All	All
Application	Postgresql	Postgresql	8.4.5	All	All	All
Application	Postgresql	Postgresql	8.4.6	All	All	All
Application	Postgresql	Postgresql	8.4.7	All	All	All
Application	Postgresql	Postgresql	8.4.8	All	All	All
Application	Postgresql	Postgresql	8.4.9	All	All	All
Application	Postgresql	Postgresql	9.0	All	All	All
Application	Postgresql	Postgresql	9.0.1	All	All	All

[illegible]

Application	Postgresql	Postgresql	8.4.4	All	All	All
Application	Postgresql	Postgresql	8.4.5	All	All	All
Application	Postgresql	Postgresql	8.4.6	All	All	All
Application	Postgresql	Postgresql	8.4.7	All	All	All
Application	Postgresql	Postgresql	8.4.8	All	All	All
Application	Postgresql	Postgresql	8.4.9	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:12.04:-: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:8.4:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.1:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.10:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.11:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.12:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.13:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.14:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.15:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.16:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.2:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.3:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.4:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.5:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.6:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.7:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.8:~::~:
cpe:2.3:a:postgresql:postgresql:8.4.9:~::~:
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:8.4:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:8.4.1:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:8.4.10:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:8.4.11:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:8.4.12:*:*:*:*:*:
cpe:2.3:a:postgresql:postgresql:8.4.13:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql:8.4.14:*****:
cpe:2.3:a:postgresql:postgresql:8.4.15:*****:
cpe:2.3:a:postgresql:postgresql:8.4.16:*****:
cpe:2.3:a:postgresql:postgresql:8.4.2:*****:
cpe:2.3:a:postgresql:postgresql:8.4.3:*****:
cpe:2.3:a:postgresql:postgresql:8.4.4:*****:
cpe:2.3:a:postgresql:postgresql:8.4.5:*****:
cpe:2.3:a:postgresql:postgresql:8.4.6:*****:
cpe:2.3:a:postgresql:postgresql:8.4.7:*****:
cpe:2.3:a:postgresql:postgresql:8.4.8:*****:
cpe:2.3:a:postgresql:postgresql:8.4.9:*****:
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 →](#)