

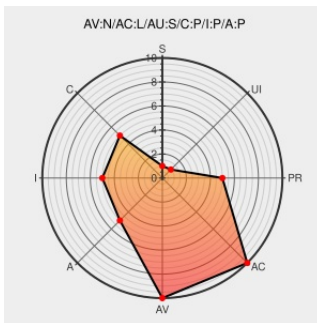


CVE-2014-2669

Published on: 03/28/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:57 PM UTC

CVE-2014-2669

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

Certain versions of [Postgresql](#) from [Postgresql](#) contain the following vulnerability:

Multiple integer overflows in contrib/hstore/hstore_io.c in PostgreSQL 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact via vectors related to the (1) hstore_recv, (2) hstore_from_arrays, and (3) hstore_from_array functions in

contrib/hstore/hstore_io.c; and the (4) hstoreArrayToPairs function in contrib/hstore/hstore_op.c, which triggers a buffer overflow. NOTE: this issue was SPLIT from CVE-2014-0064 because it has a different set of affected versions.

CVE-2014-2669 has been assigned by [M](#) cve@mitre.org 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
Debian -- Security Information -- DSA-2865-1 postgresql-9.1	www.debian.org Deprecated Link text/html	@ DEBIAN DSA-2865
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0469
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0221

Inactive Link Not Archived

PostgreSQL: Security Information	www.postgresql.org text/html	 CONFIRM www.postgresql.org/support/security/
PostgreSQL: PostgreSQL 9.3.3, 9.2.7, 9.1.12, 9.0.16 and 8.4.20 released!	Vendor Advisory www.postgresql.org text/html	 CONFIRM www.postgresql.org/about/news/1506/
Predict integer overflow to avoid buffer overruns. · postgres/postgres@31400a6 · GitHub	github.com text/html	 CONFIRM github.com/postgres/postgres/commit/31400a673325147e1205326008e32135a78
Debian -- Security Information -- DSA-2864-1 postgresql-8.4	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2864
20140220securityrelease - PostgreSQL wiki	Vendor Advisory wiki.postgresql.org text/html	 CONFIRM wiki.postgresql.org/wiki/20140220securityrelease

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
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	9.0.13	All	All	All
Application	Postgresql	Postgresql	9.0.14	All	All	All
Application	Postgresql	Postgresql	9.0.15	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	9.1.10	All	All	All
Application	Postgresql	Postgresql	9.1.11	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	9.1.9	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	9.2.4	All	All	All
Application	Postgresql	Postgresql	9.2.5	All	All	All
Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.2	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	9.0.13	All	All	All
Application	Postgresql	Postgresql	9.0.14	All	All	All
Application	Postgresql	Postgresql	9.0.15	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	9.1.10	All	All	All
Application	Postgresql	Postgresql	9.1.11	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	9.1.9	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	9.2.4	All	All	All
Application	Postgresql	Postgresql	9.2.5	All	All	All
Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
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:9.0.13:*:*:*:*:*:						
cpe:2.3:a:postgresql:postgresql:9.0.14:*:*:*:*:*:						
cpe:2.3:a:postgresql:postgresql:9.0.15:*:*:*:*:*:						
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:9.1.10:*****:
cpe:2.3:a:postgresql:postgresql:9.1.11:*****:
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:9.1.9:*****:
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:9.2.4:*****:
cpe:2.3:a:postgresql:postgresql:9.2.5:*****:
cpe:2.3:a:postgresql:postgresql:9.3:*****:
cpe:2.3:a:postgresql:postgresql:9.3.1:*****:
cpe:2.3:a:postgresql:postgresql:9.3.2:*****:
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:9.0.13:*****:
cpe:2.3:a:postgresql:postgresql:9.0.14:*****:
cpe:2.3:a:postgresql:postgresql:9.0.15:*****:
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:9.1.10:*****:
cpe:2.3:a:postgresql:postgresql:9.1.11:*****:
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:9.1.9:*****:
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:9.2.4:*****:
cpe:2.3:a:postgresql:postgresql:9.2.5:*****:
cpe:2.3:a:postgresql:postgresql:9.3:*****:
cpe:2.3:a:postgresql:postgresql:9.3.1:*****:
cpe:2.3:a:postgresql:postgresql:9.3.2:*****:

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](#)