



CVE-2017-7484

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

Summary

CVE	CVE-2017-7484
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-12 19:29:00 UTC
Updated	2018-01-05 02:31:00 UTC
Description	It was found that some selectivity estimation functions in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.10	All	All	All
Application	Postgresql	Postgresql	9.3.11	All	All	All
Application	Postgresql	Postgresql	9.3.12	All	All	All
Application	Postgresql	Postgresql	9.3.13	All	All	All
Application	Postgresql	Postgresql	9.3.14	All	All	All
Application	Postgresql	Postgresql	9.3.15	All	All	All
Application	Postgresql	Postgresql	9.3.16	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
Application	Postgresql	Postgresql	9.3.3	All	All	All
Application	Postgresql	Postgresql	9.3.4	All	All	All
Application	Postgresql	Postgresql	9.3.5	All	All	All
Application	Postgresql	Postgresql	9.3.6	All	All	All
Application	Postgresql	Postgresql	9.3.7	All	All	All
Application	Postgresql	Postgresql	9.3.8	All	All	All
Application	Postgresql	Postgresql	9.3.9	All	All	All

Application	Postgresql	Postgresql	9.4	All	All	All
Application	Postgresql	Postgresql	9.4.1	All	All	All
Application	Postgresql	Postgresql	9.4.10	All	All	All
Application	Postgresql	Postgresql	9.4.11	All	All	All
Application	Postgresql	Postgresql	9.4.2	All	All	All
Application	Postgresql	Postgresql	9.4.3	All	All	All
Application	Postgresql	Postgresql	9.4.4	All	All	All
Application	Postgresql	Postgresql	9.4.5	All	All	All
Application	Postgresql	Postgresql	9.4.6	All	All	All
Application	Postgresql	Postgresql	9.4.7	All	All	All
Application	Postgresql	Postgresql	9.4.8	All	All	All
Application	Postgresql	Postgresql	9.4.9	All	All	All
Application	Postgresql	Postgresql	9.5	All	All	All
Application	Postgresql	Postgresql	9.5.1	All	All	All
Application	Postgresql	Postgresql	9.5.2	All	All	All
Application	Postgresql	Postgresql	9.5.3	All	All	All
Application	Postgresql	Postgresql	9.5.4	All	All	All
Application	Postgresql	Postgresql	9.5.5	All	All	All
Application	Postgresql	Postgresql	9.5.6	All	All	All
Application	Postgresql	Postgresql	9.6	All	All	All
Application	Postgresql	Postgresql	9.6.1	All	All	All
Application	Postgresql	Postgresql	9.6.2	All	All	All
Application	Postgresql	Postgresql	9.3	All	All	All
Application	Postgresql	Postgresql	9.3.1	All	All	All
Application	Postgresql	Postgresql	9.3.10	All	All	All
Application	Postgresql	Postgresql	9.3.11	All	All	All
Application	Postgresql	Postgresql	9.3.12	All	All	All
Application	Postgresql	Postgresql	9.3.13	All	All	All
Application	Postgresql	Postgresql	9.3.14	All	All	All
Application	Postgresql	Postgresql	9.3.15	All	All	All
Application	Postgresql	Postgresql	9.3.16	All	All	All
Application	Postgresql	Postgresql	9.3.2	All	All	All
Application	Postgresql	Postgresql	9.3.3	All	All	All
Application	Postgresql	Postgresql	9.3.4	All	All	All
Application	Postgresql	Postgresql	9.3.5	All	All	All

Application	Postgresql	Postgresql	9.3.6	All	All	All
Application	Postgresql	Postgresql	9.3.7	All	All	All
Application	Postgresql	Postgresql	9.3.8	All	All	All
Application	Postgresql	Postgresql	9.3.9	All	All	All
Application	Postgresql	Postgresql	9.4	All	All	All
Application	Postgresql	Postgresql	9.4.1	All	All	All
Application	Postgresql	Postgresql	9.4.10	All	All	All
Application	Postgresql	Postgresql	9.4.11	All	All	All
Application	Postgresql	Postgresql	9.4.2	All	All	All
Application	Postgresql	Postgresql	9.4.3	All	All	All
Application	Postgresql	Postgresql	9.4.4	All	All	All
Application	Postgresql	Postgresql	9.4.5	All	All	All
Application	Postgresql	Postgresql	9.4.6	All	All	All
Application	Postgresql	Postgresql	9.4.7	All	All	All
Application	Postgresql	Postgresql	9.4.8	All	All	All
Application	Postgresql	Postgresql	9.4.9	All	All	All
Application	Postgresql	Postgresql	9.5	All	All	All
Application	Postgresql	Postgresql	9.5.1	All	All	All
Application	Postgresql	Postgresql	9.5.2	All	All	All
Application	Postgresql	Postgresql	9.5.3	All	All	All
Application	Postgresql	Postgresql	9.5.4	All	All	All
Application	Postgresql	Postgresql	9.5.5	All	All	All
Application	Postgresql	Postgresql	9.5.6	All	All	All
Application	Postgresql	Postgresql	9.6	All	All	All
Application	Postgresql	Postgresql	9.6.1	All	All	All
Application	Postgresql	Postgresql	9.6.2	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

References
Reference
PostgreSQL: 2017-05-11 Security Update Release
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
PostgreSQL CVE-2017-7484 Information Disclosure Vulnerability

PostgreSQL: Multiple vulnerabilities (GLSA 201710-06) — Gentoo Security

Debian -- Security Information -- DSA-3851-1 postgresql-9.4

PostgreSQL Bugs Let Remote Users Access and Modify Data in Transit and Let Remote Authenticated Users Obtain Password and Other Po

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500545 Alpine Linux Security Update for postgresql

502014 Alpine Linux Security Update for postgresql14

502782 Alpine Linux Security Update for postgresql15

504314 Alpine Linux Security Update for postgresql14

710344 Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 201710-06)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)