



CVE-2017-7486

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

Summary

CVE	CVE-2017-7486
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	PostgreSQL versions 8.4 - 9.6 are vulnerable to information leak in pg_user_mappings view which discloses foreign server

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	8.4.17	All	All	All
Application	Postgresql	Postgresql	8.4.18	All	All	All
Application	Postgresql	Postgresql	8.4.19	All	All	All
Application	Postgresql	Postgresql	8.4.2	All	All	All
Application	Postgresql	Postgresql	8.4.20	All	All	All
Application	Postgresql	Postgresql	8.4.21	All	All	All
Application	Postgresql	Postgresql	8.4.22	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
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	9.0.16	All	All	All
Application	Postgresql	Postgresql	9.0.17	All	All	All
Application	Postgresql	Postgresql	9.0.18	All	All	All
Application	Postgresql	Postgresql	9.0.19	All	All	All
Application	Postgresql	Postgresql	9.0.2	All	All	All
Application	Postgresql	Postgresql	9.0.20	All	All	All
Application	Postgresql	Postgresql	9.0.21	All	All	All
Application	Postgresql	Postgresql	9.0.22	All	All	All
Application	Postgresql	Postgresql	9.0.23	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	9.1.12	All	All	All

[illegible]

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	9.5.7	All	All	All
Application	Postgresql	Postgresql	9.6	All	All	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	8.4.17	All	All	All
Application	Postgresql	Postgresql	8.4.18	All	All	All
Application	Postgresql	Postgresql	8.4.19	All	All	All
Application	Postgresql	Postgresql	8.4.2	All	All	All
Application	Postgresql	Postgresql	8.4.20	All	All	All
Application	Postgresql	Postgresql	8.4.21	All	All	All
Application	Postgresql	Postgresql	8.4.22	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

[illegible]

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	9.3.17	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	9.4.12	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	9.5.7	All	All	All
Application	Postgresql	Postgresql	9.6	All	All	All

References

Reference
PostgreSQL: 2017-05-11 Security Update Release
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
PostgreSQL CVE-2017-7486 Information Disclosure Vulnerability
Red Hat Customer Portal
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)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report