



CVE-2009-4136

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2009-4136
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-15 18:30:01 UTC
Updated	2026-04-23 00:35:47 UTC
Description	PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.12 are vulnerable to a buffer overflow in the postgresql_fdw module. An attacker with database access could cause a denial of service or execute arbitrary code.

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	7.4.1	All	All	All

[illegible]

Application	Postgresql	Postgresql	8.0.19	All	All	All
Application	Postgresql	Postgresql	8.0.2	All	All	All
Application	Postgresql	Postgresql	8.0.20	All	All	All
Application	Postgresql	Postgresql	8.0.21	All	All	All
Application	Postgresql	Postgresql	8.0.22	All	All	All
Application	Postgresql	Postgresql	8.0.3	All	All	All
Application	Postgresql	Postgresql	8.0.4	All	All	All
Application	Postgresql	Postgresql	8.0.5	All	All	All
Application	Postgresql	Postgresql	8.0.6	All	All	All
Application	Postgresql	Postgresql	8.0.7	All	All	All
Application	Postgresql	Postgresql	8.0.8	All	All	All
Application	Postgresql	Postgresql	8.0.9	All	All	All
Application	Postgresql	Postgresql	8.1.0	All	All	All
Application	Postgresql	Postgresql	8.1.1	All	All	All
Application	Postgresql	Postgresql	8.1.10	All	All	All
Application	Postgresql	Postgresql	8.1.11	All	All	All
Application	Postgresql	Postgresql	8.1.12	All	All	All
Application	Postgresql	Postgresql	8.1.13	All	All	All
Application	Postgresql	Postgresql	8.1.14	All	All	All
Application	Postgresql	Postgresql	8.1.15	All	All	All
Application	Postgresql	Postgresql	8.1.16	All	All	All
Application	Postgresql	Postgresql	8.1.17	All	All	All
Application	Postgresql	Postgresql	8.1.18	All	All	All
Application	Postgresql	Postgresql	8.1.2	All	All	All
Application	Postgresql	Postgresql	8.1.3	All	All	All
Application	Postgresql	Postgresql	8.1.4	All	All	All
Application	Postgresql	Postgresql	8.1.5	All	All	All
Application	Postgresql	Postgresql	8.1.6	All	All	All
Application	Postgresql	Postgresql	8.1.7	All	All	All
Application	Postgresql	Postgresql	8.1.8	All	All	All
Application	Postgresql	Postgresql	8.1.9	All	All	All
Application	Postgresql	Postgresql	8.2	All	All	All
Application	Postgresql	Postgresql	8.2.1	All	All	All
Application	Postgresql	Postgresql	8.2.10	All	All	All
Application	Postgresql	Postgresql	8.2.11	All	All	All

Application	Postgresql	Postgresql	8.2.12	All	All	All
Application	Postgresql	Postgresql	8.2.13	All	All	All
Application	Postgresql	Postgresql	8.2.14	All	All	All
Application	Postgresql	Postgresql	8.2.2	All	All	All
Application	Postgresql	Postgresql	8.2.3	All	All	All
Application	Postgresql	Postgresql	8.2.4	All	All	All
Application	Postgresql	Postgresql	8.2.5	All	All	All
Application	Postgresql	Postgresql	8.2.6	All	All	All
Application	Postgresql	Postgresql	8.2.7	All	All	All
Application	Postgresql	Postgresql	8.2.8	All	All	All
Application	Postgresql	Postgresql	8.2.9	All	All	All
Application	Postgresql	Postgresql	8.3.1	All	All	All
Application	Postgresql	Postgresql	8.3.2	All	All	All
Application	Postgresql	Postgresql	8.3.3	All	All	All
Application	Postgresql	Postgresql	8.3.4	All	All	All
Application	Postgresql	Postgresql	8.3.5	All	All	All
Application	Postgresql	Postgresql	8.3.6	All	All	All
Application	Postgresql	Postgresql	8.3.7	All	All	All
Application	Postgresql	Postgresql	8.3.8	All	All	All
Application	Postgresql	Postgresql	8.4.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	

References
Reference
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 8.2.15
SecurityFocus
'[security bulletin] HPSBMU02781 SSRT100617 rev.1 - HP Network Node Manager i (NNMi) for HP-UX, Linux' - MARC
Support
Webmail- OVH
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 8.3.9
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 8.1.19
PostgreSQL Index Function Session State Modification Local Privilege Escalation Vulnerability
osvdb.org/61039

Support / Security / Advisories / / MDVSA-2009:333 Mandriva								
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 8.0.23								
Support								
[SECURITY] Fedora 11 Update: postgresql-8.3.9-1.fc11								
Red Hat update for postgresql - Secunia.com								
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:001								
wiki.rpath.com/wiki/Advisories:rPSA-2010-0012								
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 7.4.27								
Bug 546321 – CVE-2009-4136 postgresql: SQL privilege escalation via modifications to session-local state								
SecurityTracker.com Archives - PostgreSQL Index Function State Changing Flaw Lets Remote Authenticated Users Gain Elevated Privileges								
Support								
PostgreSQL: Security Information								
PostgreSQL SSL Certificate Processing and Privilege Escalation Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com								
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH								
PostgreSQL: Documentation: Manuals: PostgreSQL 8.4: Release 8.4.2								
[SECURITY] Fedora 12 Update: postgresql-8.4.2-1.fc12								
Repository / Oval Repository								
CVE Program record								
NVD vulnerability detail								
Vendor Comments And Credit								
<table><tr><th>Organization</th><th>Published</th><th>Contributor</th><th>Statement</th></tr><tr><td>Red Hat</td><td>2010-05-20</td><td>Mark Cox</td><td>This issue was addressed in Red Hat Enterprise Linux 3 via https://rhn.redhat.com/errata/RHSA</td></tr></table>	Organization	Published	Contributor	Statement	Red Hat	2010-05-20	Mark Cox	This issue was addressed in Red Hat Enterprise Linux 3 via https://rhn.redhat.com/errata/RHSA
Organization	Published	Contributor	Statement					
Red Hat	2010-05-20	Mark Cox	This issue was addressed in Red Hat Enterprise Linux 3 via https://rhn.redhat.com/errata/RHSA					
There are currently no legacy QID mappings associated with this CVE.								