



# CVE-2009-3231

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

## Summary

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-3231                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                 |
| <b>Assigner</b>        | cve@mitre.org                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                           |
| <b>Published</b>       | 2009-09-17 10:30:00 UTC                                                                                                |
| <b>Updated</b>         | 2018-10-10 19:43:00 UTC                                                                                                |
| <b>Description</b>     | The core server component in PostgreSQL 8.3 before 8.3.8 and 8.2 before 8.2.14, when using LDAP authentication with ar |

## Risk And Classification

### Problem Types: CWE-287

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| 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 | 8.2.2   | 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     | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.1   | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.2   | All    | All     | All      |

|             |                            |                            |        |     |     |     |
|-------------|----------------------------|----------------------------|--------|-----|-----|-----|
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.3  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.4  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.5  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.6  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.7  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2    | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.1  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.10 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.11 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.12 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.13 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.2  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.3  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.4  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.5  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.6  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.7  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.8  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.2.9  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3    | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.1  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.2  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.3  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.4  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.5  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.6  | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.3.7  | All | All | All |

| References                                                                                                    |  |  |  |  |         |                         |
|---------------------------------------------------------------------------------------------------------------|--|--|--|--|---------|-------------------------|
| Reference                                                                                                     |  |  |  |  | Source  | Link                    |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:016                                            |  |  |  |  | SUSE    | <a href="#">lists.o</a> |
| '[security bulletin] HPSBMU02781 SSRT100617 rev.1 - HP Network Node Manager i (NNMi) for HP-UX, Linux' - MARC |  |  |  |  | HP      | <a href="#">marc.i</a>  |
| PostgreSQL Multiple Security Vulnerabilities                                                                  |  |  |  |  | BID     | <a href="#">www.s</a>   |
| [SECURITY] Fedora 11 Update: postgresql-8.3.8-1.fc11                                                          |  |  |  |  | FEDORA  | <a href="#">www.r</a>   |
| Bug 522084 – CVE-2009-3231 postgresql: LDAP authentication bypass when anonymous LDAP bind are allowed        |  |  |  |  | CONFIRM | <a href="#">bugzill</a> |
| PostgreSQL Database Manager: Multiple SQL Injection Vulnerabilities                                           |  |  |  |  | CONFIRM |                         |

|                                                                                                             |         |                          |
|-------------------------------------------------------------------------------------------------------------|---------|--------------------------|
| PostgreSQL: Documentation: Manuals: PostgreSQL 8.3: Release 8.3.8                                           | CONFIRM | <a href="#">www.p</a>    |
| Fedora update for postgresql - Secunia Advisories - Vulnerability Information - Secunia.com                 | SECUNIA | <a href="#">secuni</a>   |
| [SECURITY] Fedora 10 Update: postgresql-8.3.8-1.fc10                                                        | FEDORA  | <a href="#">www.r</a>    |
| USN-834-1: PostgreSQL vulnerabilities   Ubuntu                                                              | UBUNTU  | <a href="#">www.u</a>    |
| Security Advisory SA36800 - Ubuntu update for postgresql - Secunia                                          | SECUNIA | <a href="#">secuni</a>   |
| Debian update for postgresql - Secunia Advisories - Vulnerability Information - Secunia.com                 | SECUNIA | <a href="#">secuni</a>   |
| wiki.rpath.com/wiki/Advisories:rPSA-2010-0012                                                               | CONFIRM | <a href="#">wiki.rp</a>  |
| PostgreSQL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com          | SECUNIA | <a href="#">secuni</a>   |
| PostgreSQL: Security Information                                                                            | CONFIRM | <a href="#">www.p</a>    |
| SecurityFocus                                                                                               | BUGTRAQ | <a href="#">www.s</a>    |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:017                                          | SUSE    | <a href="#">lists.og</a> |
| Debian -- Security Information -- DSA-1900-1 postgresql-7.4, postgresql-8.1, postgresql-8.3, postgresql-8.4 | DEBIAN  | <a href="#">www.u</a>    |
| CVE Program record                                                                                          | CVE.ORG | <a href="#">www.c</a>    |
| NVD vulnerability detail                                                                                    | NVD     | <a href="#">nvd.ni</a>   |

#### Vendor Comments And Credit

| Organization | Published  | Contributor | Statement                                                                                      |
|--------------|------------|-------------|------------------------------------------------------------------------------------------------|
| Red Hat      | 2009-09-24 | Tomas Hoger | Not vulnerable. This issue did not affect the versions of PostgreSQL as shipped with Red Hat E |

There are currently no legacy QID mappings associated with this CVE.

© 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](#)