



# CVE-2006-5541

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

## Summary

|                        |                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2006-5541                                                                                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                                                |
| <b>Published</b>       | 2006-10-26 17:07:00 UTC                                                                                                                                                                     |
| <b>Updated</b>         | 2023-10-12 13:28:00 UTC                                                                                                                                                                     |
| <b>Description</b>     | backend/parser/parse_coerce.c in PostgreSQL 7.4.1 through 7.4.14, 8.0.x before 8.0.9, and 8.1.x before 8.1.5 allows remote attackers to execute arbitrary SQL commands via a crafted query. |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Postgresql | Postgresql | All     | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.1   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.10  | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.11  | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.12  | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.13  | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.14  | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.2   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.3   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.4   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.5   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.6   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.7   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.8   | All    | All     | All      |
| Application | Postgresql | Postgresql | 7.4.9   | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.0     | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.0.1   | All    | All     | All      |

[illegible]

|             |                            |                            |       |     |     |     |
|-------------|----------------------------|----------------------------|-------|-----|-----|-----|
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.1   | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.1.1 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.1.2 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.1.3 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 8.1.4 | All | All | All |

References

| Reference                                                                                             | Source   | Link                            |
|-------------------------------------------------------------------------------------------------------|----------|---------------------------------|
| Ubuntu update for postgresql - Advisories - Secunia                                                   | SECUNIA  | <a href="#">secunia.com</a>     |
| ASA-2007-117 (RHSA-2007-0067)                                                                         | CONFIRM  | <a href="#">support.avaya</a>   |
| PostgreSQL Denial of Service Vulnerabilities - Advisories - Secunia                                   | SECUNIA  | <a href="#">secunia.com</a>     |
| usn/usn-369-2 - Ubuntu: Linux for human beings                                                        | UBUNTU   | <a href="#">www.ubuntu.c</a>    |
| Security update for PostgreSQL                                                                        | CONFIRM  | <a href="#">support.novell.</a> |
| Security Announcement                                                                                 | SUSE     | <a href="#">www.novell.co</a>   |
| SUSE Update for Multiple Packages - Advisories - Secunia                                              | SECUNIA  | <a href="#">secunia.com</a>     |
| usn/usn-369-1 - Ubuntu: Linux for human beings                                                        | UBUNTU   | <a href="#">www.ubuntu.c</a>    |
| Repository / Oval Repository                                                                          | OVAL     | <a href="#">oval.cisecurity</a> |
| PostgreSQL Multiple Local Denial of Service Vulnerabilities                                           | BID      | <a href="#">www.securityfo</a>  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                      | VUPEN    | <a href="#">www.vupen.cc</a>    |
| 2006-0059                                                                                             | TRUSTIX  | <a href="#">www.trustix.or</a>  |
| Advisories - Mandriva Linux                                                                           | MANDRIVA | <a href="#">www.mandriva</a>    |
| Mandriva update for postgresql - Advisories - Secunia                                                 | SECUNIA  | <a href="#">secunia.com</a>     |
| Support                                                                                               | REDHAT   | <a href="#">www.redhat.cc</a>   |
| SecurityTracker.com Archives - PostgreSQL Processing Bugs Let Remote Authenticated Users Deny Service | SECTRACK | <a href="#">securitytracker</a> |
| rhn.redhat.com   Red Hat Support                                                                      | REDHAT   | <a href="#">www.redhat.cc</a>   |
| Trustix update for postgresql - Advisories - Secunia                                                  | SECUNIA  | <a href="#">secunia.com</a>     |
| Avaya Products PostgreSQL Denial of Service and Information Disclosure - Advisories - Secunia         | SECUNIA  | <a href="#">secunia.com</a>     |
| PostgreSQL: News: New PostgreSQL Minor Versions Released                                              | CONFIRM  | <a href="#">www.postgres</a>    |
| Novell update for postgresql - Advisories - Secunia                                                   | SECUNIA  | <a href="#">secunia.com</a>     |
| Redmine 404 error                                                                                     | CONFIRM  | <a href="#">projects.comm</a>   |
| CVE Program record                                                                                    | CVE.ORG  | <a href="#">www.cve.org</a>     |
| NVD vulnerability detail                                                                              | NVD      | <a href="#">nvd.nist.gov</a>    |



No vendor comments have been submitted for this CVE.

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](#)