



# CVE-2016-5423

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-5423                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2016-12-09 23:59:00 UTC                                                                                                     |
| <b>Updated</b>         | 2018-01-05 02:31:00 UTC                                                                                                     |
| <b>Description</b>     | PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote |

## Risk And Classification

### Problem Types: CWE-476

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                     | Product                      | Version | Update | Edition | Language |
|------------------|----------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>     | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>     | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2     | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.1   | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.10  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.11  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.12  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.13  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.14  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.15  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.16  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.17  | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.2   | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.3   | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.4   | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.5   | All    | All     | All      |
| Application      | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | 9.2.6   | All    | All     | All      |

| Application |            |            |        |     |     |     |
|-------------|------------|------------|--------|-----|-----|-----|
| Application | Postgresql | Postgresql | 9.2.7  | All | All | All |
| Application | Postgresql | Postgresql | 9.2.8  | All | All | All |
| Application | Postgresql | Postgresql | 9.2.9  | 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 | 9.3.2  | 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 | 9.4.2  | 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 | 9.5    | 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 | 9.2    | All | All | All |
| Application | Postgresql | Postgresql | 9.2.1  | All | All | All |
| Application | Postgresql | Postgresql | 9.2.10 | All | All | All |
| Application | Postgresql | Postgresql | 9.2.11 | All | All | All |
| Application | Postgresql | Postgresql | 9.2.12 | All | All | All |



|             |                            |                            |       |     |     |     |
|-------------|----------------------------|----------------------------|-------|-----|-----|-----|
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.4.8 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.5   | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.5.1 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.5.2 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.5.3 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | All   | All | All | All |

| References                                                                                                 |  |  |  |          |                             |  |
|------------------------------------------------------------------------------------------------------------|--|--|--|----------|-----------------------------|--|
| Reference                                                                                                  |  |  |  | Source   | Link                        |  |
| Red Hat Customer Portal                                                                                    |  |  |  | REDHAT   | <a href="#">rhn.redhat.</a> |  |
| Red Hat Customer Portal                                                                                    |  |  |  | REDHAT   | <a href="#">rhn.redhat.</a> |  |
| PostgreSQL CVE-2016-5423 NULL Pointer Dereference Remote Code Execution Vulnerability                      |  |  |  | BID      | <a href="#">www.secu</a>    |  |
| Red Hat Customer Portal                                                                                    |  |  |  | REDHAT   | <a href="#">rhn.redhat.</a> |  |
| PostgreSQL: Documentation: 9.6: Release 9.4.9                                                              |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| Red Hat Customer Portal                                                                                    |  |  |  | REDHAT   | <a href="#">access.red</a>  |  |
| PostgreSQL: Multiple vulnerabilities (GLSA 201701-33) — Gentoo security                                    |  |  |  | GENTOO   | <a href="#">security.ge</a> |  |
| PostgreSQL: Documentation: 9.6: Release 9.5.4                                                              |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| Bug 1364001 – CVE-2016-5423 postgresql: CASE/WHEN with inlining can cause untrusted pointer dereference    |  |  |  | CONFIRM  | <a href="#">bugzilla.re</a> |  |
| PostgreSQL Bugs Let Remote Authenticated Users Deny Service and Gain Elevated Privileges - SecurityTracker |  |  |  | SECTRACK | <a href="#">www.secu</a>    |  |
| Red Hat Customer Portal                                                                                    |  |  |  | REDHAT   | <a href="#">rhn.redhat.</a> |  |
| PostgreSQL: 2016-08-11 Security Update Release                                                             |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| PostgreSQL: Documentation: 9.6: Release 9.3.14                                                             |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| PostgreSQL: Documentation: 9.6: Release 9.2.18                                                             |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| Debian -- Security Information -- DSA-3646-1 postgresql-9.4                                                |  |  |  | DEBIAN   | <a href="#">www.debia</a>   |  |
| PostgreSQL: Documentation: 9.6: Release 9.1.23                                                             |  |  |  | CONFIRM  | <a href="#">www.postg</a>   |  |
| CVE Program record                                                                                         |  |  |  | CVE.ORG  | <a href="#">www.cve.o</a>   |  |
| NVD vulnerability detail                                                                                   |  |  |  | NVD      | <a href="#">nvd.nist.go</a> |  |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings |                                                                   |
|---------------------|-------------------------------------------------------------------|
| 710501              | Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 201701-33) |

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)