



# CVE-2012-3488

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-3488                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2012-10-03 21:55:00 UTC                                                                                                        |
| <b>Updated</b>         | 2016-12-08 03:02:00 UTC                                                                                                        |
| <b>Description</b>     | The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 |

## Risk And Classification

### Problem Types: CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Postgresql | Postgresql | 8.3     | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.1   | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.10  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.11  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.12  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.13  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.14  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.15  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.16  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.17  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.18  | All    | All     | All      |
| Application | Postgresql | Postgresql | 8.3.19  | 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 | 8.3.9  | 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 | 8.4.2  | 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 | 9.0.2  | 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 | 9.1    | All | All | All |
| Application | Postgresql | Postgresql | 9.1.1  | All | All | All |
| Application | Postgresql | Postgresql | 9.1.2  | All | All | All |
| Application | Postgresql | Postgresql | 9.1.3  | All | All | All |
| Application | Postgresql | Postgresql | 9.1.4  | All | All | All |
| Application | Postgresql | Postgresql | 8.3    | All | All | All |
| Application | Postgresql | Postgresql | 8.3.1  | All | All | All |
| Application | Postgresql | Postgresql | 8.3.10 | All | All | All |
| Application | Postgresql | Postgresql | 8.3.11 | All | All | All |
| Application | Postgresql | Postgresql | 8.3.12 | All | All | All |



|             |                            |                            |       |     |     |     |
|-------------|----------------------------|----------------------------|-------|-----|-----|-----|
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.0.7 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.0.8 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.1   | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.1.1 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.1.2 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.1.3 | All | All | All |
| Application | <a href="#">Postgresql</a> | <a href="#">Postgresql</a> | 9.1.4 | All | All | All |

## References

| Reference                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------|
| Multiple vulnerabilities in PostgreSQL (Third Party Vulnerability Resolution Blog)                                                     |
| openSUSE-SU-2012:1251-1: moderate: postgresql, postgresql-libs                                                                         |
| PostgreSQL: Documentation: 8.3: Release 8.3.20                                                                                         |
| Security Advisory SA50636 - Red Hat update for postgresql - Secunia                                                                    |
| Support / Security / Advisories / / MDVSA-2012:139   Mandriva                                                                          |
| About Secunia Research   Flexera                                                                                                       |
| Debian -- Security Information -- DSA-2534-1 postgresql-8.4                                                                            |
| Red Hat Customer Portal                                                                                                                |
| Red Hat Customer Portal                                                                                                                |
| Security Advisory SA50946 - Oracle Solaris PostgreSQL &quot;xml_parse()&quot; and &quot;xslt_process()&quot; Vulnerabilities - Secunia |
| PostgreSQL 'xslt_process()' Function Arbitrary File Creation or Overwrite Vulnerability                                                |
| PostgreSQL: Security Information                                                                                                       |
| openSUSE-SU-2012:1288-1: moderate: postgresql, postgresql-libs                                                                         |
| APPLE-SA-2013-03-14-1 OS X Mountain Lion v10.8.3 and Security Update 2013-001                                                          |
| PostgreSQL: Documentation: 9.0: Release 9.0.9                                                                                          |
| PostgreSQL: Security Update 2012-08-17 released                                                                                        |
| USN-1542-1: PostgreSQL vulnerabilities   Ubuntu                                                                                        |
| Bug 849172 – CVE-2012-3488 postgresql (xml2 contrib module): XXE by applying XSL stylesheet to the document                            |
| Security Advisory SA50635 - Red Hat update for postgresql and postgresql84 - Secunia                                                   |
| openSUSE-SU-2012:1299-1: moderate: postgresql: security and bugfix upgra                                                               |
| PostgreSQL: Documentation: 9.1: Release 9.1.5                                                                                          |
| PostgreSQL: Documentation: 8.4: Release 8.4.13                                                                                         |
| Security Advisory SA50718 - SUSE update for postgresql and postgresql-libs - Secunia                                                   |
| Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView                                             |
| CVE Program record                                                                                                                     |
| NVD vulnerability detail                                                                                                               |

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](#)