



# CVE-2007-3278

Published on: 06/19/2007 12:00:00 AM UTC

Last Modified on: 02/24/2023 03:35:00 PM UTC

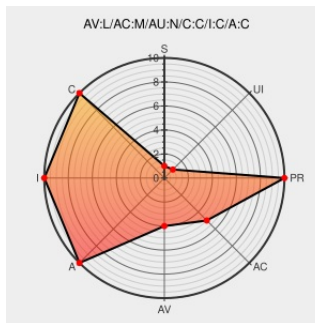
## CVE-2007-3278

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

PostgreSQL 8.1 and probably later versions, when local trust authentication is enabled and the Database Link library (dblink) is installed, allows remote attackers to access arbitrary accounts and execute arbitrary SQL queries via a dblink host parameter that proxies the connection from 127.0.0.1.

CVE-2007-3278 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access Vector

LOCAL

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

COMPLETE

Availability Impact

COMPLETE

## CVE References

Description

Tags

Link

Red Hat update for postgresql - Advisories - Secunia

[Vendor Advisory](#)  
[web.archive.org](#)  
[text/html](#)

[X](#) SECUNIA 28438

Advisories | Mandriva

[www.mandriva.com](#)  
[text/html](#)

[MANDRIVA MDKSA-2007:188](#)

No Description Provided

[sunsolve.sun.com](#)

[SUNALERT 103197](#)

Inactive Link Not Archived

Sun Solaris 10 PostgreSQL Multiple Vulnerabilities - Advisories - Secunia

[Vendor Advisory](#)  
[web.archive.org](#)  
[text/html](#)

[X](#) SECUNIA 28437

|                                                                                                        |                                                                                                                                                                  |                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Description Provided                                                                                | <a href="https://osvdb.org">osvdb.org</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                          |  OSVDB 40899                                                                                                                                                               |
| 404 Not Found                                                                                          | <a href="http://www.portcullis.co.uk/application/pdf">www.portcullis.co.uk<br/>application/pdf</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  MISC<br><a href="http://www.portcullis.co.uk/uplds/whitepapers/Having_Fun_With_PostgreSQL.pdf">www.portcullis.co.uk/uplds/whitepapers/Having_Fun_With_PostgreSQL.pdf</a> |
| IBM X-Force Exchange                                                                                   | <a href="https://exchange.xforce.ibmcloud.com/text/html">exchange.xforce.ibmcloud.com<br/>text/html</a>                                                          |  XF postgresql-dblink-sql-injection(35142)                                                                                                                                |
| No Description Provided                                                                                | <a href="http://h20000.www2.hp.com">h20000.www2.hp.com</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                         |  HP SSRT080006                                                                                                                                                            |
| Gentoo Linux Documentation -<br>- PostgreSQL: Multiple<br>vulnerabilities                              | <a href="https://security.gentoo.org/text/html">security.gentoo.org<br/>text/html</a>                                                                            |  GENTOO GLSA-200801-15                                                                                                                                                    |
| SecurityFocus                                                                                          | <a href="http://www.securityfocus.com/text/html">www.securityfocus.com<br/>text/html</a>                                                                         |  BUGTRAQ 20070616 Having Fun With PostgreSQL                                                                                                                              |
| Support                                                                                                | <a href="http://www.redhat.com/text/html">www.redhat.com<br/>text/html</a>                                                                                       |  REDHAT RHSA-2008:0040                                                                                                                                                    |
| Debian update for postgresql -<br>Advisories - Secunia                                                 | <a href="#">Vendor Advisory</a><br><a href="http://web.archive.org/text/html">web.archive.org<br/>text/html</a>                                                  |  SECUNIA 28454                                                                                                                                                            |
| Debian -- Security Information<br>-- DSA-1463-1 postgresql-7.4                                         | <a href="http://www.debian.org/text/html">www.debian.org<br/>text/html</a><br><a href="#">Deprecated Link</a>                                                    |  DEBIAN DSA-1463                                                                                                                                                          |
| USN-568-1: PostgreSQL<br>vulnerabilities   Ubuntu security<br>notices                                  | <a href="http://usn.ubuntu.com/text/html">usn.ubuntu.com<br/>text/html</a>                                                                                       |  UBUNTU USN-568-1                                                                                                                                                       |
| rhn.redhat.com   Red Hat<br>Support                                                                    | <a href="http://www.redhat.com/text/html">www.redhat.com<br/>text/html</a>                                                                                       |  REDHAT RHSA-2008:0038                                                                                                                                                  |
|                                                                                                        | <a href="http://www.leidecker.info/text/plain">www.leidecker.info<br/>text/plain</a>                                                                             |  MISC <a href="http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt">www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt</a>                          |
| Red Hat update for postgresql<br>- Advisories - Secunia                                                | <a href="#">Vendor Advisory</a><br><a href="http://web.archive.org/text/html">web.archive.org<br/>text/html</a>                                                  |  SECUNIA 28445                                                                                                                                                          |
| Repository / Oval Repository                                                                           | <a href="http://oval.cisecurity.org/text/html">oval.cisecurity.org<br/>text/html</a>                                                                             |  OVAL oval:org.mitre.oval:def:10334                                                                                                                                     |
| SecurityFocus                                                                                          | <a href="http://www.securityfocus.com/text/html">www.securityfocus.com<br/>text/html</a>                                                                         |  BUGTRAQ 20070618 Re: Having Fun With PostgreSQL                                                                                                                        |
| No Description Provided                                                                                | <a href="http://sunsolve.sun.com">sunsolve.sun.com</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                             |  SUNALERT 200559                                                                                                                                                        |
| Ubuntu update for postgresql -<br>Advisories - Secunia                                                 | <a href="#">Vendor Advisory</a><br><a href="http://web.archive.org/text/html">web.archive.org<br/>text/html</a>                                                  |  SECUNIA 28477                                                                                                                                                          |
| HP Internet Express for Tru64<br>UNIX Multiple PostgreSQL<br>Vulnerabilities - Advisories -<br>Secunia | <a href="http://web.archive.org/text/html">web.archive.org<br/>text/html</a>                                                                                     |  SECUNIA 29638                                                                                                                                                          |
| Support   Red Hat                                                                                      | <a href="http://www.redhat.com/text/html">www.redhat.com<br/>text/html</a>                                                                                       |  REDHAT RHSA-2008:0039                                                                                                                                                  |

|                                                                                                |                                                                                                 |                                                                                                       |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Gentoo update for postgresql - Advisories - Secunia                                            | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a> |  SECUNIA 28679        |
| Debian update for postgresql-7.4 - Advisories - Secunia                                        | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a> |  SECUNIA 28479       |
| Debian -- Security Information -- DSA-1460-1 postgresql-8.1                                    | <a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a>  |  DEBIAN DSA-1460     |
| Mandriva update for postgresql - Secunia Advisories - Vulnerability Intelligence - Secunia.com | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a> |  SECUNIA 28376       |
| Webmail - OVH                                                                                  | <a href="#">www.vupen.com</a><br><a href="#">text/html</a>                                      |  VUPEN ADV-2008-1071 |
| Webmail - OVH                                                                                  | <a href="#">www.vupen.com</a><br><a href="#">text/html</a>                                      |  VUPEN ADV-2008-0109 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                        | Vendor                     | Product                      | Version | Update | Edition | Language |
|-------------------------------------------------------------|----------------------------|------------------------------|---------|--------|---------|----------|
| Operating System                                            | <a href="#">Debian</a>     | <a href="#">Debian Linux</a> | 3.1     | All    | All     | All      |
| Operating System                                            | <a href="#">Debian</a>     | <a href="#">Debian Linux</a> | 4.0     | All    | All     | All      |
| Application                                                 | <a href="#">Postgresql</a> | <a href="#">Postgresql</a>   | All     | All    | All     | All      |
| 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     | All    | All     | All      |
| <a href="#">cpe:2.3:o:debian:debian_linux:3.1:*****:*</a>   |                            |                              |         |        |         |          |
| <a href="#">cpe:2.3:o:debian:debian_linux:4.0:*****:*</a>   |                            |                              |         |        |         |          |
| <a href="#">cpe:2.3:a:postgresql:postgresql:*****:*</a>     |                            |                              |         |        |         |          |
| <a href="#">cpe:2.3:a:postgresql:postgresql:8.1:*****:*</a> |                            |                              |         |        |         |          |
| <a href="#">cpe:2.3:a:postgresql:postgresql:8.1:*****:*</a> |                            |                              |         |        |         |          |

© [CVE.report](#) 2023   |

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)