



CVE-2007-2138

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

Summary

CVE	CVE-2007-2138
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-24 20:19:00 UTC
Updated	2018-10-19 18:54:00 UTC
Description	Untrusted search path vulnerability in PostgreSQL before 7.3.19, 7.4.x before 7.4.17, 8.0.x before 8.0.13, 8.1.x before 8.1.9

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

References

Reference	Source	Link
Webmail OVH- OVH	VUPEN	www.vupen
Red Hat update for postgresql - Advisories - Secunia	SECUNIA	secunia.c

Gentoo Linux Documentation -- PostgreSQL: Privilege escalation	GENTOO	security.g
ASA-2007-190 (RHSA-2007-0336 and RHSA-2007-0337)	CONFIRM	support.a
IBM X-Force Exchange	XF	exchange
Repository / Oval Repository	OVAL	oval.cisec
PostgreSQL Lets Remote Authenticated Users Gain Elevated SQL Privileges - SecurityTracker	SECTrack	www.seci
Support	REDHAT	www.redh
Advisories - Mandriva Linux	MANDRIVA	www.mar
Ubuntu update for postgresql - Advisories - Secunia	SECUNIA	secunia.c
#200713: Security Vulnerability in PostgreSQL SECURITY DEFINER Functions May Allow Escalation of Privileges	SUNALERT	sunsolve.
rPath update for postgresql and postgresql-server - Advisories - Secunia	SECUNIA	secunia.c
issues.rpath.com/browse/RPL-1292	CONFIRM	issues.rpa
Debian -- Security Information -- DSA-1309-1 postgresql-8.1	DEBIAN	www.deb
rhn.redhat.com Red Hat Support	REDHAT	rhn.redha
PostgreSQL SECURITY DEFINER Functions Privilege Escalation - Advisories - Secunia	SECUNIA	secunia.c
Sun Solaris PostgreSQL SECURITY DEFINER Privilege Escalation - Advisories - Secunia	SECUNIA	secunia.c
Mandriva update for postgresql - Advisories - Secunia	SECUNIA	secunia.c
2007-0015	TRUSTIX	www.trus
Debian update for postgresql-8.1 - Advisories - Secunia	SECUNIA	secunia.c
Debian update for libexif - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
Trustix update for postgresql - Advisories - Secunia	SECUNIA	secunia.c
PostgreSQL: News: Security Update Releases	CONFIRM	www.posi
Debian -- Security Information -- DSA-1311-1 postgresql-7.4	DEBIAN	www.deb
PostgreSQL: Security Information	CONFIRM	www.posi
Debian update for postgresql-7.4 - Advisories - Secunia	SECUNIA	secunia.c
PostgreSQL SECURITY DEFINER Function Local Privilege Escalation Vulnerability	BID	www.seci
Webmail OVH- OVH	VUPEN	www.vup
Avaya Products PostgreSQL SECURITY DEFINER Privilege Escalation - Advisories - Secunia	SECUNIA	secunia.c
Gentoo update for postgresql - Advisories - Secunia	SECUNIA	secunia.c
USN-454-1: PostgreSQL vulnerability Ubuntu	UBUNTU	www.ubu
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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](#)