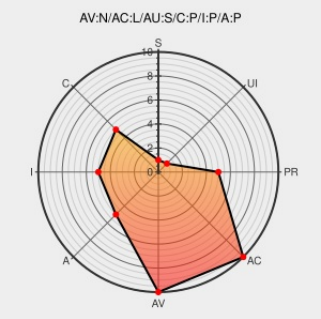
CVE-2002-1401

Published on: 01/08/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1401

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Postgresql from Postgresql contain the following vulnerability:

Buffer overflows in (1) circle_poly, (2) path_encode and (3) path_add (also incorrectly identified as path_addr) for PostgreSQL 7.2.3 and earlier allow attackers to cause a denial of service and possibly execute arbitrary code, possibly as a result of an integer overflow.

CVE-2002-1401 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
@(#)Mordre Labs advisory 0x0005: Several buffer overruns in PostgreSQL	Vendor Advisory, archives.postgresql.org, text/html	MISC archives.postgresql.org/pgsql-hackers/2002-08/msg02047.php
Re: @(#)Mordre Labs advisory 0x0005: Several buffer overruns in PostgreS	archives.postgresql.org, text/html	MISC archives.postgresql.org/pgsql-hackers/2002-08/msg02081.php
redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2003:001
Secunia - Advisories - Mandrake updates to postgresql	web.archive.org, text/html	SECUNIA 8034
Home - Conectiva	distro.conectiva.com.br, text/html	CONECTIVA CLA-2002:524
Debian -- Security Information -- DSA-165-1 postgresql	Patch	DEBIAN DSA-165

Vendor Advisory
www.debian.org
Depreciated Link
text/html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	6.3.2	All	All	All
Application	Postgresql	Postgresql	6.5.3	All	All	All
Application	Postgresql	Postgresql	7.0.3	All	All	All
Application	Postgresql	Postgresql	7.1	All	All	All
Application	Postgresql	Postgresql	7.1.1	All	All	All
Application	Postgresql	Postgresql	7.1.2	All	All	All
Application	Postgresql	Postgresql	7.1.3	All	All	All
Application	Postgresql	Postgresql	7.2	All	All	All
Application	Postgresql	Postgresql	7.2.1	All	All	All
Application	Postgresql	Postgresql	7.2.2	All	All	All
Application	Postgresql	Postgresql	7.2.3	All	All	All
Application	Postgresql	Postgresql	6.3.2	All	All	All
Application	Postgresql	Postgresql	6.5.3	All	All	All
Application	Postgresql	Postgresql	7.0.3	All	All	All
Application	Postgresql	Postgresql	7.1	All	All	All
Application	Postgresql	Postgresql	7.1.1	All	All	All
Application	Postgresql	Postgresql	7.1.2	All	All	All
Application	Postgresql	Postgresql	7.1.3	All	All	All
Application	Postgresql	Postgresql	7.2	All	All	All
Application	Postgresql	Postgresql	7.2.1	All	All	All
Application	Postgresql	Postgresql	7.2.2	All	All	All
Application	Postgresql	Postgresql	7.2.3	All	All	All

cpe:2.3:a:postgresql:postgresql:6.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:postgresql:postgresql:7.0.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:6.3.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:6.5.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.0.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.1.3:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.1:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.2:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:7.2.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→