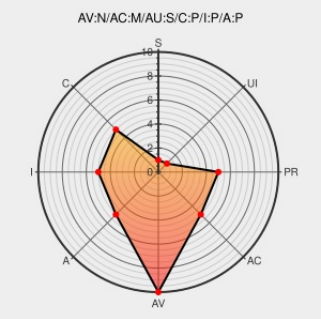
CVE-2010-3781

Published on: 10/06/2010 12:00:00 AM UTC

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

CVE-2010-3781

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



Certain versions of Pl/php from Alvaro Herrera contain the following vulnerability:

The PL/php add-on 1.4 and earlier for PostgreSQL does not properly protect script execution by a different SQL user identity within the same session, which allows remote authenticated users to gain privileges via crafted script code in a SECURITY DEFINER function, a related issue to CVE-2010-3433.

CVE-2010-3781 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6 - MEDIUM

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

CVE References

Description	Tags	Link
PostgreSQL: Documentation: Manuals: PostgreSQL 9.0: Release 9.0.1	www.postgresql.org text/html	MISC www.postgresql.org/docs/9.0/static/release-9-0-1.html
PostgreSQL: News: PostgreSQL 2010-10-05 Security Update	web.archive.org text/html Inactive Link Not Archived	MISC www.postgresql.org/about/news.1244
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6645

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	Alvaro Herrera	Pl/php	1.0	All	All	All
Application	Alvaro Herrera	Pl/php	1.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.3	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.5	beta1	All	All
Application	Alvaro Herrera	Pl/php	All	All	All	All
Application	Alvaro Herrera	Pl/php	1.0	All	All	All
Application	Alvaro Herrera	Pl/php	1.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.3	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.5	beta1	All	All
Application	Alvaro Herrera	Pl/php	1.0	All	All	All
Application	Alvaro Herrera	Pl/php	1.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.1	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.2	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.3	All	All	All
Application	Alvaro Herrera	Pl/php	1.3.5	beta1	All	All
Application	Alvaro Herrera	Pl/php	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

cpe:2.3:a:alvaro_herrera:pl/php:1.0:*:*:*:*:*:*:*

cpe:2.3:a:alvaro_herrera:pl/php:1.1:*:*:*:*:*:*:*

cpe:2.3:a:alvaro_herrera:pl/php:1.2:*:*:*:*:*:*:*

cpe:2.3:a:alvaro_herrera:pl/php:1.3.1:*:*:*:*:*:*:*

cpe:2.3:a:alvaro_herrera:pl/php:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl/php:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl/php:1.3.5:beta1:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl/php:*:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.5:beta1:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:1.3.5:beta1:*:*:*:*:*:*:

cpe:2.3:a:alvaro_herrera:pl\/php:*:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report