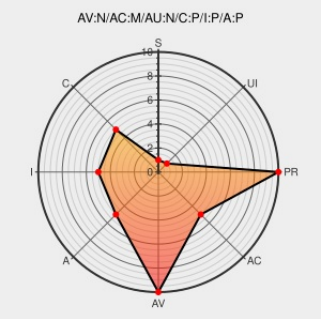
CVE-2009-3422

Published on: 09/25/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:25 PM UTC

CVE-2009-3422

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



Certain versions of Paoliber from Zenas contain the following vulnerability:

login.php in Zenas PaoLiber 1.1, when register_globals is enabled, allows remote attackers to bypass authentication and gain administrative access by setting the login_ok parameter to 1.

CVE-2009-3422 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PaoLink/PaoBacheca/PaoLiber Authentication Bypass Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory, web.archive.org, text/html	SECUNIA 36023
No Description Provided	Exploit, www.osvdb.org, Inactive Link, Not Archived	OSVDB 56758
PaoLiber 1.1 (login_ok) Authentication Bypass Vulnerability	www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 9294

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	Zenas	Paoliber	1.1	All	All	All
Application	Zenas	Paoliber	1.1	All	All	All

cpe:2.3:a:zenas:paoliber:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:zenas:paoliber:1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→