



CVE-2009-3421

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

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

CVE-2009-3421

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Pao-bacheca Guestbook](#) from [Zenas](#) contain the following vulnerability:

login.php in Zenas PaoBacheca Guestbook 2.1, when register_globals is enabled, allows remote attackers to bypass authentication and gain administrative access by setting the login_ok parameter to 1.

CVE-2009-3421 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

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](#)

[X](#) [SECUNIA 36023](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF](#)
[paobachecaguestbook-login-sec-bypass\(52100\)](#)

No Description Provided

[Exploit](#)
[www.osvdb.org](#)

[OSVDB 56757](#)

Inactive Link **Not Archived**

PaoBacheca Guestbook 2.1 (login_ok) Auth Bypass Vulnerability

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 9293](#)

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	Zenas	Pao-bacheca Guestbook	2.1	All	All	All
Application	Zenas	Pao-bacheca Guestbook	2.1	All	All	All
cpe:2.3:a:zenas:pao-bacheca_guestbook:2.1:*****:						
cpe:2.3:a:zenas:pao-bacheca_guestbook:2.1:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →