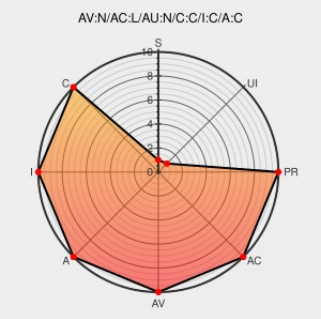
CVE-2004-0261

Published on: 09/01/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0261

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



Certain versions of Openjournal from Openjournal contain the following vulnerability:

oj.cgi in OpenJournal 2.0 through 2.0.5 allows remote attackers to bypass authentication and access the control panel via a 0 in the uid parameter.

CVE-2004-0261 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
'Open Journal Blog Authenticaion Bypassing Vulnerability' - MARC	marc.info text/html	BUGTRAQ 20040206 Open Journal Blog Authenticaion Bypassing Vulnerability
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 3872
	www.grohol.com text/plain	CONFIRM www.grohol.com/downloads/oj/latest/changelog.txt
OpenJournal Authentication Bypassing Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 9598
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF openjournal-uid-admin-access(15069)

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	Openjournal	Openjournal	2.0	All	All	All
Application	Openjournal	Openjournal	2.0_1	All	All	All
Application	Openjournal	Openjournal	2.0_2	All	All	All
Application	Openjournal	Openjournal	2.0_3	All	All	All
Application	Openjournal	Openjournal	2.0_4	All	All	All
Application	Openjournal	Openjournal	2.0_5	All	All	All
Application	Openjournal	Openjournal	2.0	All	All	All
Application	Openjournal	Openjournal	2.0_1	All	All	All
Application	Openjournal	Openjournal	2.0_2	All	All	All
Application	Openjournal	Openjournal	2.0_3	All	All	All
Application	Openjournal	Openjournal	2.0_4	All	All	All
Application	Openjournal	Openjournal	2.0_5	All	All	All

cpe:2.3:a:openjournal:openjournal:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_1:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_2:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_3:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_4:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_5:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_1:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_2:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_3:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_4:*:*:*:*:*:*:*:

cpe:2.3:a:openjournal:openjournal:2.0_5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→