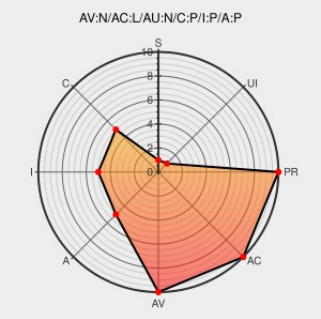
CVE-2006-3249

Published on: 06/27/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:58 PM UTC

CVE-2006-3249

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



Certain versions of Phorum from Phorum contain the following vulnerability:

** DISPUTED ** SQL injection vulnerability in search.php in Phorum 5.1.14 and earlier allows remote attackers to execute arbitrary SQL commands via the page parameter. NOTE: the vendor has disputed this report, stating "If a non positive integer or non-integer is used for the page parameter for a search URL, the search query will use a negative number for the LIMIT clause. This causes the query to break, showing no results. It IS NOT however a sql injection error." While the original report is from a researcher with mixed accuracy, as of 20060703, CVE does not have any additional information regarding this issue.

CVE-2006-3249 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
404 Not Found	www.phorum.org text/html Inactive Link Not Archived	MISC www.phorum.org/cgi-bin/trac.cgi/ticket/382#preview
Phorum Support Forums :: Phorum Development	www.phorum.org text/html	MISC www.phorum.org/phorum5/read.php?14,114358
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phorum-search-page-sql-injection(27369)

Page not found	pridels0.blogspot.com text/html Inactive Link Not Archived	MISC pridels0.blogspot.com/2006/06/phorum-sql-injection-vuln.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 27165

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	Phorum	Phorum	All	All	All	All

cpe:2.3:a:phorum:phorum:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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