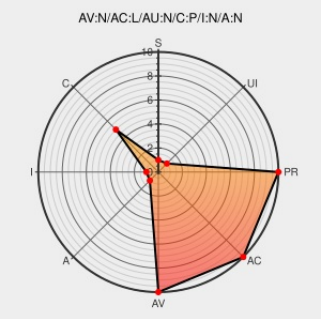
CVE-2004-1579

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1579

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



Certain versions of Cubecart from Devellion contain the following vulnerability:

index.php in CubeCart 2.0.1 allows remote attackers to gain sensitive information via an HTTP request with an invalid cat_id parameter, which reveals the full path in a PHP error message.

CVE-2004-1579 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF cubecart-catid-path-disclosure(17630)
'Full path disclosure and sql injection on CubeCart 2.0.1' - MARC	marc.info text/html	BUGTRAQ 20041006 Full path disclosure and sql injection on CubeCart 2.0.1

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	Devellion	Cubecart	2.0.1	All	All	All
Application	Devellion	Cubecart	2.0.1	All	All	All

cpe:2.3:a:devellion:cubecart:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:devellion:cubecart:2.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→