



CVE-2003-0275

Published on: 05/14/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

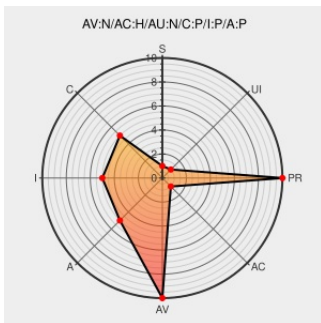
CVE-2003-0275

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Yabb](#) from [Yabb](#) contain the following vulnerability:
SSI.php in YaBB SE 1.5.2 allows remote attackers to execute arbitrary PHP code by modifying the sourcedir parameter to reference a URL on a remote web server that contains the code.

CVE-2003-0275 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

'II-Labs Advisory: Remote code execution in YaBBse 1.5.2 (php version)' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20030509 II-Labs Advisory: Remote code execution in YaBBse 1.5.2 \(php version\)](#)

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	Yabb	Yabb	1.5.2	All	second_edition	All
Application	Yabb	Yabb	1.5.2	All	second_edition	All
cpe:2.3:a:yabb:yabb:1.5.2:*:second_edition:*****:						
cpe:2.3:a:yabb:yabb:1.5.2:*:second_edition:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		