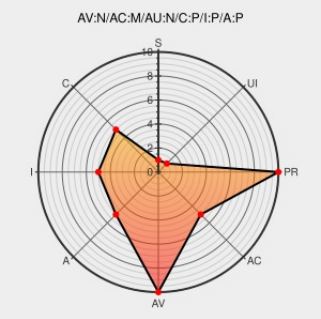
CVE-2003-1256

Published on: 12/31/2003 05:00:00 AM UTC

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

CVE-2003-1256

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



Certain versions of E-theni from E-theni contain the following vulnerability:

aff_liste_langue.php in E-theni allows remote attackers to execute arbitrary PHP code by modifying the rep_include parameter to reference a URL on a remote web server that contains para_langue.php.

CVE-2003-1256 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
ISS X-Force Database:etheni-afflistelangue-file-include(11013): E-theni aff_liste_langue.php script could allow an attacker to include remote PHP files	web.archive.org, text/html, Inactive Link, Not Archived	XF etheni-afflistelangue-file-include(11013)
SecurityFocus	Exploit, Patch, www.securityfocus.com, text/html	BUGTRAQ 20030106 E-theni (PHP)
No Description Provided	Exploit, Patch, web.archive.org, text/html, Inactive Link, Not Archived	VULNWATCH 20030106 E-theni (PHP)
E-theni Remote Include Command Execution Vulnerability	Exploit	BID 6970

E-theni Remote Include Command Execution Vulnerability

cve.report (archive)

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	E-theni	E-theni	All	All	All	All
Application	E-theni	E-theni	All	All	All	All

cpe:2.3:a:e-theni:e-theni:*:*:*:*:*:*:*:*:

cpe:2.3:a:e-theni:e-theni:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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