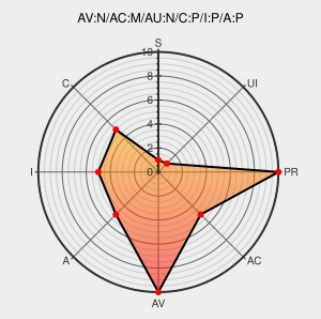
CVE-2006-6426

Published on: 12/10/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:04 PM UTC

CVE-2006-6426

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



Certain versions of Thinkedit from Thinkedit contain the following vulnerability:

PHP remote file inclusion vulnerability in design/thinkedit/render.php in ThinkEdit 1.9.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the template_file parameter.

CVE-2006-6426 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
ThinkEdit "template_file" File Inclusion Vulnerability - Advisories - Secunia	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 23279
ThinkEdit Include File Bug in 'render.php' Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com, text/html	SECTRACK 1017359
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF thinkedit-render-file-include(30772)
500 Internal Server Error	Patch, svn.berlios.de, text/html, Inactive Link, Not Archived	CONFIRM svn.berlios.de/viewcvs/thinkedit/trunk/design/thinkedit/render.php?rev=321&r1=230&r2=321

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-4906
ThinkEdit 1.9.2 (render.php) Remote File Inclusion Vulnerability	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 2898

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	Thinkedit	Thinkedit	All	All	All	All

cpe:2.3:a:thinkedit:thinkedit:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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