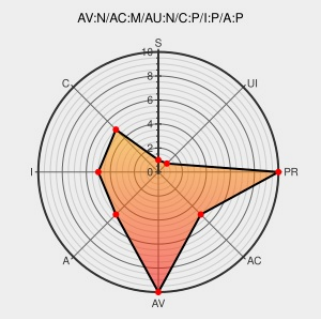
CVE-2007-5314

Published on: 10/09/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:38 PM UTC

CVE-2007-5314

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



Certain versions of Xkiosk Web from Xkiosk contain the following vulnerability:

PHP remote file inclusion vulnerability in system/funcs/xkurl.php in xKiosk WEB 3.0.1i, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the PEARPATH parameter.

CVE-2007-5314 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
xKiosk 3.0.1i - 'xkurl.php?PEARPATH' Remote File Inclusion - PHP webapps Exploit	www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 4502
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF xkioskweb-xkurl-file-include(37030)
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 37620
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2007-3427
xKiosk WEB "PEARPATH" Remote File Inclusion Vulnerability - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 27140

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	Xkiosk	Xkiosk Web	3.0.1i	All	All	All
Application	Xkiosk	Xkiosk Web	3.0.1i	All	All	All

cpe:2.3:a:xkiosk:xkiosk_web:3.0.1i:*:*:*:*:*:*:*:

cpe:2.3:a:xkiosk:xkiosk_web:3.0.1i:*:*:*:*:*:*:*:

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