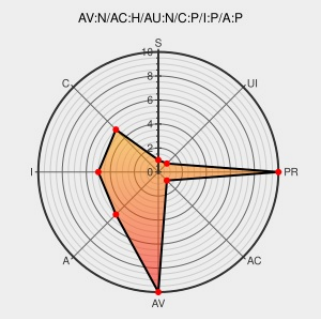
CVE-2006-1480

Published on: 03/28/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1480

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



Certain versions of Webalbum from Duda contain the following vulnerability:

Directory traversal vulnerability in start.php in WebAlbum 2.02 allows remote attackers to include arbitrary files and execute commands by (1) injecting code into local log files via GET commands, then (2) accessing that log via a .. (dot dot) sequence and a trailing null (%00) byte in the skin2 COOKIE parameter.

CVE-2006-1480 has been assigned by 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF webalbum-skin2-parameter-file-include(25443)
WEBalbum Local File Inclusion Vulnerability - Advisories - Secunia	Exploit, Vendor Advisory, web.archive.org, text/html	SECUNIA 19400
WEBalbum Remote Command Execution Vulnerability	Exploit, cve.report (archive), text/html	BID 17228
WebAlbum <= 2.02pl COOKIE[skin2] Remote Code Execution Exploit	www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 1608

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1108
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24160

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	Duda	Webalbum	All	All	All	All

cpe:2.3:a:duda:webalbum:*:*:*:*:*:*:*:*:

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