



CVE-2009-4927

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-4927
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-07-12 13:27:00 UTC
Updated	2017-09-19 01:30:00 UTC
Description	WB News 2.1.2 allows remote attackers to bypass authentication and gain administrative access via a modified WBNEWS

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webmobo	Wbnews	2.1.2	All	All	All
Application	Webmobo	Wbnews	2.1.2	All	All	All

References

Reference	Source	Link
WB News 2.1.2 - Insecure Cookie Handling - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com/exploits/12121/
WB News Insecure Cookie Handling Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com/advisories/41441/
WB News Insecure Cookie Authentication Bypass Vulnerability	BID	www.securityfocus.com/bid/37441/
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve-2009-4927
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2009-4927

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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 registered 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](#).

Free CVE JSON API cve.report/api

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