



CVE-2014-9367

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-9367
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-31 21:59:00 UTC
Updated	2015-01-03 01:28:00 UTC
Description	Incomplete blacklist vulnerability in the urlencode function in lib/TWiki.pm in TWiki 6.0.0 and 6.0.1 allows remote attackers to

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Twiki	Twiki	6.0.0	All	All	All
Application	Twiki	Twiki	6.0.1	All	All	All
Application	Twiki	Twiki	6.0.0	All	All	All
Application	Twiki	Twiki	6.0.1	All	All	All

References

Reference	Source
TWiki Input Validation Flaw in WebSearch Topic Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK
Full Disclosure: TWiki Security Alert CVE-2014-9367: XSS Vulnerability with Scope and Other URL Parameters of WebSearch	FULLDISC
TWiki 6.0.0 / 6.0.1 WebSearch Cross Site Scripting ≈ Packet Storm	MISC
SecurityAlert-CVE-2014-9367 < Codev < TWiki	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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 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](#)