



CVE-2014-7237

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

Summary

CVE	CVE-2014-7237
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-16 00:55:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	lib/TWiki/Sandbox.pm in TWiki 6.0.0 and earlier, when running on Windows, allows remote attackers to bypass intended ac

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Twiki	Twiki	All	All	All	All

References

Reference

- Full Disclosure: TWiki Security Alert CVE-2014-7237: Apache configuration file upload on TWiki on Windows server
- SecurityAlert-CVE-2014-7237 < Codev < TWiki
- IBM X-Force Exchange
- Twiki 'Sandbox.pm' File Validation Flaw Lets Remote Authenticated Users Upload Arbitrary Windows Apache Configuration Files - SecurityTr
- CVE Program record
- NVD vulnerability detail

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](#)