



CVE-2011-1838

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

Summary

CVE	CVE-2011-1838
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-20 22:55:00 UTC
Updated	2018-10-09 19:32:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in TemplateLogin.pm in TWiki before 5.0.2 allow remote attackers to inject

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Twiki	Twiki	4.0.0	All	All	All
Application	Twiki	Twiki	4.0.1	All	All	All
Application	Twiki	Twiki	4.0.2	All	All	All
Application	Twiki	Twiki	4.0.3	All	All	All
Application	Twiki	Twiki	4.0.4	All	All	All
Application	Twiki	Twiki	4.0.5	All	All	All
Application	Twiki	Twiki	4.1.0	All	All	All
Application	Twiki	Twiki	4.1.1	All	All	All
Application	Twiki	Twiki	4.1.2	All	All	All
Application	Twiki	Twiki	4.2.0	All	All	All
Application	Twiki	Twiki	4.2.1	All	All	All
Application	Twiki	Twiki	4.2.2	All	All	All
Application	Twiki	Twiki	4.2.3	All	All	All
Application	Twiki	Twiki	4.2.4	All	All	All
Application	Twiki	Twiki	4.3.0	All	All	All
Application	Twiki	Twiki	4.3.1	All	All	All
Application	Twiki	Twiki	4.3.2	All	All	All

Application	Twiki	Twiki	4.5.0	All	All	All
Application	Twiki	Twiki	5.0.0	All	All	All
Application	Twiki	Twiki	4.0.0	All	All	All
Application	Twiki	Twiki	4.0.1	All	All	All
Application	Twiki	Twiki	4.0.2	All	All	All
Application	Twiki	Twiki	4.0.3	All	All	All
Application	Twiki	Twiki	4.0.4	All	All	All
Application	Twiki	Twiki	4.0.5	All	All	All
Application	Twiki	Twiki	4.1.0	All	All	All
Application	Twiki	Twiki	4.1.1	All	All	All
Application	Twiki	Twiki	4.1.2	All	All	All
Application	Twiki	Twiki	4.2.0	All	All	All
Application	Twiki	Twiki	4.2.1	All	All	All
Application	Twiki	Twiki	4.2.2	All	All	All
Application	Twiki	Twiki	4.2.3	All	All	All
Application	Twiki	Twiki	4.2.4	All	All	All
Application	Twiki	Twiki	4.3.0	All	All	All
Application	Twiki	Twiki	4.3.1	All	All	All
Application	Twiki	Twiki	4.3.2	All	All	All
Application	Twiki	Twiki	4.5.0	All	All	All
Application	Twiki	Twiki	5.0.0	All	All	All
Application	Twiki	Twiki	All	All	All	All

References

Reference	Source	Link
SecurityFocus	BUGTRAQ	www.securityfocus.com
Twiki 'origurl' Parameter Cross Site Scripting Vulnerability	BID	www.securityfocus.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Twiki Input Validation Flaw in the 'origurl' Parameter Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	securitytracker.com
XSS vulnerability in Twiki < 5.0.2 - SecurityReason.com	SREASON	securityreason.com
Netsparker, False Positive Free Web Application Security Scanner - Mavituna Security	MISC	www.mavitunasecurity.com
Twiki "origurl" Cross-Site Scripting Vulnerability - Secunia.com	SECUNIA	secunia.com
SecurityAlert-CVE-2011-1838 < Codev < Twiki	CONFIRM	twiki.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)