# 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.securityfocu |
| TWiki 'origurl' Parameter Cross Site Scripting Vulnerability | BID | www.securityfocu |
| 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.c |
| XSS vulnerability in TWiki < 5.0.2 - SecurityReason.com | SREASON | securityreason.c |
| Netsparker, False Positive Free Web Application Security Scanner - Mavituna Security | MISC | www.mavitunase |
| 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.



**Free CVE JSON API** cve.report/api

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