



# CVE-2014-0977

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

## Summary

<b>CVE</b>	CVE-2014-0977
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-01-10 17:55:00 UTC
<b>Updated</b>	2017-08-29 01:34:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Rich Text Editor in Movable Type 5.0x, 5.1x before 5.161, 5.2.x before 5.2.9, a

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sixapart	Movabletype	5.0	rc2	All	All
Application	Sixapart	Movabletype	5.01	All	All	All
Application	Sixapart	Movabletype	5.02	All	All	All
Application	Sixapart	Movabletype	5.03	All	All	All
Application	Sixapart	Movabletype	5.031	All	All	All
Application	Sixapart	Movabletype	5.04	All	All	All
Application	Sixapart	Movabletype	5.11	All	All	All
Application	Sixapart	Movabletype	5.12	All	All	All
Application	Sixapart	Movabletype	5.13	All	All	All
Application	Sixapart	Movabletype	5.14	All	All	All
Application	Sixapart	Movabletype	5.15	All	All	All
Application	Sixapart	Movabletype	5.2	All	All	All
Application	Sixapart	Movabletype	5.2.2	All	All	All
Application	Sixapart	Movabletype	5.2.3	All	All	All
Application	Sixapart	Movabletype	5.2.6	All	All	All
Application	Sixapart	Movabletype	5.2.7	All	All	All
Application	Sixapart	Movabletype	6.0	All	All	All

Application	Sixapart	Movabletype	5.0	rc2	All	All
Application	Sixapart	Movabletype	5.01	All	All	All
Application	Sixapart	Movabletype	5.02	All	All	All
Application	Sixapart	Movabletype	5.03	All	All	All
Application	Sixapart	Movabletype	5.031	All	All	All
Application	Sixapart	Movabletype	5.04	All	All	All
Application	Sixapart	Movabletype	5.11	All	All	All
Application	Sixapart	Movabletype	5.12	All	All	All
Application	Sixapart	Movabletype	5.13	All	All	All
Application	Sixapart	Movabletype	5.14	All	All	All
Application	Sixapart	Movabletype	5.15	All	All	All
Application	Sixapart	Movabletype	5.2	All	All	All
Application	Sixapart	Movabletype	5.2.2	All	All	All
Application	Sixapart	Movabletype	5.2.3	All	All	All
Application	Sixapart	Movabletype	5.2.6	All	All	All
Application	Sixapart	Movabletype	5.2.7	All	All	All
Application	Sixapart	Movabletype	6.0	All	All	All

## References

Reference	Source	L
oss-sec: CVE Request: cross-site scripting vulnerabilities in movable type 6.0.1, 5.2.9, and 5.161	MLIST	sc
Security Advisory SA56295 - Movable Type Rich Text Editor Script Insertion Vulnerability - Secunia	SECUNIA	sc
oss-sec: Re: CVE Request: cross-site scripting vulnerabilities in movable type 6.0.1, 5.2.9, and 5.161	MLIST	sc
Security Advisory SA56405 - Debian update for movabletype-opensource - Secunia	SECUNIA	sc
MovableType.org – News: Movable Type 6.0.1, 5.2.9, and 5.161 Released to Close Security Vulnerabilities	CONFIRM	nr
Movable Type Input Validation Flaw in Editor Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	w
Multiple Movable Type Products Multiple HTML Injection Vulnerabilities	BID	w
#734304 - movabletype-opensource: XSS Security vulnerabilities fixed in 5.2.9 (CVE-2014-0977) - Debian Bug report logs	CONFIRM	bl
Debian -- Security Information -- DSA-2841-1 movabletype-opensource	DEBIAN	w
IBM X-Force Exchange	XF	e:
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nr

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](#)