



CVE-2013-1123

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

Summary

CVE	CVE-2013-1123
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-15 12:09:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the server in Cisco Unified MeetingPlace 7.0 allow remote attackers to i

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Meetingplace	7.0	All	All	All
Application	Cisco	Unified Meetingplace	7.0	All	All	All

References

Reference	Source	Link
Alert Details - Security Center - Cisco Systems	CONFIRM	tools.cisco
90075	OSVDB	osvdb.org
Cisco Unified MeetingPlace CVE-2013-1123 Unspecified Cross Site Scripting Vulnerability	BID	www.secu
Security Advisory SA52109 - Cisco Unified MeetingPlace Web Interface Cross-Site Scripting Vulnerability - Secunia	SECUNIA	secunia.c
Cisco Security Notice: Cisco Unified MeetingPlace Server Cross-Site Scripting Vulnerability	CISCO	tools.cisco
IBM X-Force Exchange	XF	exchange
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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](#)