



CVE-2012-1302

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

Summary

CVE	CVE-2012-1302
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-28 02:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in amMap 2.6.3 allow remote attackers to inject arbitrary web script or HTML

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ammap Project	Ammap	2.6.3	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
Flash Exploitation Database				
Trend Micro InterScan Messaging Security Virtual Appliance Input Validation Flaw in 3rd Party 'amMap' Component Lets Remote Users Cond				
Critical Patch 1670 to resolve third-party module XSS vulnerability - IMSVA				
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.				