



CVE-2011-5240

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

Summary

CVE	CVE-2011-5240
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-06 12:21:26 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Magento 1.5 and 1.6.2 does not verify that the server hostname matches a domain name in the subject's Common Name (C

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Magentocommerce	Magento	1.5	All	All	All

Application	Magentocommerce	Magento	1.6.2	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference	Source		Link			
#PeerJacking - SSL Ecosystem Attacks Against Online Commerce unrest.ca	af854a3a-2127-422b-91ae-364da2661108		www.unrest.ca			
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.						