CVE-2012-0329

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-0329
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-19 15:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco Digital Media Manager 5.2.2 and earlier, and 5.2.3, allows remote authenticated users to execute arbitrary code via v

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

Problem Types: CWE-94 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Digital Media Manager	3.5	All	All	All

Application	Cisco	Digital Media Manager	3.5\(1\)	All	All	All
Application	Cisco	Digital Media Manager	4.0	All	All	All
Application	Cisco	Digital Media Manager	4.1\(0\)40	All	All	All
Application	Cisco	Digital Media Manager	5.0	All	All	All
Application	Cisco	Digital Media Manager	5.0.2	All	All	All
Application	Cisco	Digital Media Manager	5.0.3	All	All	All
Application	Cisco	Digital Media Manager	5.1	All	All	All
Application	Cisco	Digital Media Manager	5.1.1	All	All	All
Application	Cisco	Digital Media Manager	5.2.1	All	All	All
Application	Cisco	Digital Media Manager	5.2.1.1	All	All	All
Application	Cisco	Digital Media Manager	5.2.3	All	All	All
Application	Cisco	Digital Media Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Cisco Digital Media Manager Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364c
Cisco Security Advisory: Cisco Digital Media Manager Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364c
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.