CVE-2010-0573

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

Summary

CVE	CVE-2010-0573
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-05 19:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Unspecified vulnerability on the Cisco Digital Media Player before 5.2 allows remote attackers to hijack the source of (1) vid

Risk And Classification

Primary CVSS: v2.0 8.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Digital Media Player	5.2	All	All	All

Hardware	Cisco	Digital Media Player 4300g	5.2	All	All	All
Hardware	Cisco	Digital Media Player 4305g	5.2	All	All	All
Hardware	Cisco	Digital Media Player 4400g	5.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a
osvdb.org/62723	af854a3a
Cisco Digital Media Player Content Injection Vulnerability - Advisories - Community	af854a3a
SecurityTracker.com Archives - Cisco Digital Media Player Lets Remote Users Inject Arbitrary Video and Data Content	af854a3a
Cisco Security Advisory: Cisco Digital Media Player Remote Display Unauthorized Content Injection Vulnerability - Cisco Systems	af854a3a
Cisco Digital Media Player Video or Data Content Injection Vulnerability	af854a3a
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.