CVE-2009-0062

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

Summary

CVE	CVE-2009-0062
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-05 00:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in the Cisco Wireless LAN Controller (WLC), Cisco Catalyst 6500 Wireless Services Module (WiSM

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-264 | 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
Hardware	Cisco	Catalyst 3750 Series Integrated Wireless Lan Controller	4.2	All	All	All

Hardware	Cisco	Catalyst 3750 Series Integrated Wireless Lan Controller	4.2.173.0	All	All	All
Hardware	Cisco	Catalyst 6500 Wireless Services Modules	4.2	All	All	All
Hardware	Cisco	Catalyst 6500 Wireless Services Modules	4.2.173.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	4.2	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	4.2.173.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Multiple Cisco Wireless LAN Controllers Multiple Remote Vulnerabilities	af854a
Cisco Wireless LAN Controller Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	af854a
Cisco Security Advisory: Multiple Vulnerabilities in Cisco Wireless LAN Controllers [Products & Services] - Cisco Systems	af854a
Cisco Products Denial of Service and Security Bypass Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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