



CVE-2014-3291

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

Summary

CVE	CVE-2014-3291
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-08 16:55:00 UTC
Updated	2016-09-07 19:11:00 UTC
Description	Cisco Wireless LAN Controller (WLC) devices allow remote attackers to cause a denial of service (NULL pointer dereference)

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wireless Lan Controller	All	All	All	All
Hardware	Cisco	Wireless Lan Controller	All	All	All	All

References

Reference	Source
Cisco Security Notice: Cisco Wireless LAN Controller Cisco Discovery Protocol Denial of Service Vulnerability	CISCO
Alert Details - Security Center - Cisco Systems	CONFIRM
Cisco Wireless LAN Controller CVE-2014-3291 Denial of Service Vulnerability	BID
Cisco Wireless LAN Controller CDP Processing Flaw Lets Remote Users Deny Service - SecurityTracker	SECTRACK
Security Advisory SA57895 - Cisco Wireless LAN Controller Cisco Discovery Protocol Denial of Service Vulnerability - Secunia	SECUNIA
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)