



CVE-2017-12280

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

Summary

CVE	CVE-2017-12280
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-02 16:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) Discovery Request parsing functionalit

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wireless Lan Controller	-	All	All	All
Hardware	Cisco	Wireless Lan Controller	-	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	-	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	-	All	All	All

References

Reference
Cisco Wireless LAN Controller CAPWAP Discovery Request Processing Bug Lets Remote Users Cause the Target System to Reload - Security
Cisco Wireless LAN Controller CAPWAP Discovery Request Denial of Service Vulnerability
Cisco Wireless LAN Controller CVE-2017-12280 Denial of Service Vulnerability
CVE Program record
NVD vulnerability detail

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](#)