



CVE-2017-12279

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

Summary

CVE	CVE-2017-12279
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 packet processing code of Cisco IOS Software for Cisco Aironet Access Points could allow an unauth

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Aironet Ap	-	All	All	All
Hardware	Cisco	Aironet Ap	-	All	All	All
Operating System	Cisco	Aironet Ap Firmware	-	All	All	All
Operating System	Cisco	Aironet Ap Firmware	-	All	All	All

References

Reference

- Cisco IOS Software for Cisco Aironet Access Points Information Disclosure Vulnerability
- Cisco IOS for Cisco Aironet Access Points IP Packet Padding Error Lets Remote Users Obtain Potentially Sensitive Information on the Target
- Cisco IOS Software for Aironet Access Points CVE-2017-12279 Information Disclosure 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](#).

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