



CVE-2017-12274

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

Summary

CVE	CVE-2017-12274
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 Extensible Authentication Protocol (EAP) ingress frame processing for the Cisco Aironet 1560, 2800, and :

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Aironet 1562d	-	All	All	All
Hardware	Cisco	Aironet 1562d	-	All	All	All
Hardware	Cisco	Aironet 1562e	-	All	All	All
Hardware	Cisco	Aironet 1562e	-	All	All	All
Hardware	Cisco	Aironet 1562i	-	All	All	All
Hardware	Cisco	Aironet 1562i	-	All	All	All
Operating System	Cisco	Aironet 1562 Firmware	-	All	All	All
Operating System	Cisco	Aironet 1562 Firmware	-	All	All	All
Hardware	Cisco	Aironet 2800e	-	All	All	All
Hardware	Cisco	Aironet 2800e	-	All	All	All
Hardware	Cisco	Aironet 2800i	-	All	All	All
Hardware	Cisco	Aironet 2800i	-	All	All	All
Operating System	Cisco	Aironet 2800 Firmware	-	All	All	All
Operating System	Cisco	Aironet 2800 Firmware	-	All	All	All
Hardware	Cisco	Aironet 3800e	-	All	All	All
Hardware	Cisco	Aironet 3800e	-	All	All	All
Hardware	Cisco	Aironet 3800i	-	All	All	All

Hardware	Cisco	Aironet 3800i	-	All	All	All
Hardware	Cisco	Aironet 3800p	-	All	All	All
Hardware	Cisco	Aironet 3800p	-	All	All	All
Operating System	Cisco	Aironet 3800 Firmware	-	All	All	All
Operating System	Cisco	Aironet 3800 Firmware	-	All	All	All

References

Reference	Source
Cisco Aironet 1560, 2800, and 3800 Series Access Point Platforms Extensible Authentication Protocol Denial of Service Vulnerability	CONF
Cisco Aironet Access Points CVE-2017-12274 Denial of Service Vulnerability	BID
Cisco Aironet EAP Frame Processing Bug Lets Remote Users Cause the Target System to Reload - SecurityTracker	SECT
CVE Program record	CVE.C
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](#).

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