CVE-2020-3552

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-3552
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-24 18:15:00 UTC
Updated	2021-04-16 15:01:00 UTC
Description	A vulnerability in the Ethernet packet handling of Cisco Aironet Access Points (APs) Software could allow an unauthenticate

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Access Points	All	All	All	All
Operating System	Cisco	Access Points	All	All	All	All
Hardware	Cisco	Aironet 1542d	-	All	All	All
Hardware	Cisco	Aironet 1542d	-	All	All	All
Hardware	Cisco	Aironet 1542i	-	All	All	All
Hardware	Cisco	Aironet 1542i	-	All	All	All
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
Hardware	Cisco	Aironet 1810	-	All	All	All
Hardware	Cisco	Aironet 1810	-	All	All	All
Hardware	Cisco	Aironet 1815	-	All	All	All
Hardware	Cisco	Aironet 1815	-	All	All	All
Hardware	Cisco	Aironet 1830e	-	All	All	All

Hardware	Cisco	Aironet 1830e	-	All	All	All
Hardware	Cisco	Aironet 1830i	-	All	All	All
Hardware	Cisco	Aironet 1830i	-	All	All	All
Hardware	Cisco	Aironet 1840	-	All	All	All
Hardware	Cisco	Aironet 1840	-	All	All	All
Hardware	Cisco	Aironet 1850e	-	All	All	All
Hardware	Cisco	Aironet 1850e	-	All	All	All
Hardware	Cisco	Aironet 1850i	-	All	All	All
Hardware	Cisco	Aironet 1850i	-	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
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
Hardware	Cisco	Aironet 4800	-	All	All	All
Hardware	Cisco	Aironet 4800	-	All	All	All
Application	Cisco	Aironet Access Point Software	8.10\(1.255\)	All	All	All
Application	Cisco	Aironet Access Point Software	8.10\(1.255\)	All	All	All
Application	Cisco	Business Access Points	All	All	All	All
Application	Cisco	Business Access Points	All	All	All	All
Hardware	Cisco	Catalyst 9800-40	-	All	All	All
Hardware	Cisco	Catalyst 9800-40	-	All	All	All
Hardware	Cisco	Catalyst 9800-80	-	All	All	All
Hardware	Cisco	Catalyst 9800-80	-	All	All	All
Hardware	Cisco	Catalyst 9800-cl	-	All	All	All
Hardware	Cisco	Catalyst 9800-cl	-	All	All	All
Hardware	Cisco	Catalyst 9800-l	-	All	All	All
Hardware	Cisco	Catalyst 9800-l	-	All	All	All
Hardware	Cisco	Catalyst 9800-l-c	-	All	All	All
Hardware	Cisco	Catalyst 9800-l-c	-	All	All	All

Hardware	Cisco	Catalyst 9800-l-f	-	All	All	All
Hardware	Cisco	Catalyst 9800-l-f	-	All	All	All
Operating System	Cisco	Wireless Lan Controller	All	All	All	All
Operating System	Cisco	Wireless Lan Controller	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Aironet Access Points Ethernet Wired Clients Denial of Service Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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 registred 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