



CVE-2021-1565

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-1565
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-23 03:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco (

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst 9300-24p-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-24p-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-24s-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-24s-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-24t-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-24t-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-24u-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-24u-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-24ux-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-24ux-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48p-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-48p-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48s-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-48s-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48t-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-48t-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48u-a	-	All	All	All

Hardware	Cisco	Catalyst 9300-48u-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48un-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-48un-e	-	All	All	All
Hardware	Cisco	Catalyst 9300-48uxm-a	-	All	All	All
Hardware	Cisco	Catalyst 9300-48uxm-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24p-4g-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24p-4g-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24p-4x-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24p-4x-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24t-4g-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24t-4g-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24t-4x-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-24t-4x-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48p-4g-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48p-4g-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48p-4x-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48p-4x-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48t-4g-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48t-4g-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48t-4x-a	-	All	All	All
Hardware	Cisco	Catalyst 9300I-48t-4x-e	-	All	All	All
Hardware	Cisco	Catalyst 9300I Stack	-	All	All	All
Hardware	Cisco	Catalyst 9400	-	All	All	All
Hardware	Cisco	Catalyst 9400 Supervisor Engine-1	-	All	All	All
Hardware	Cisco	Catalyst 9407r	-	All	All	All
Hardware	Cisco	Catalyst 9410r	-	All	All	All
Hardware	Cisco	Catalyst 9500	-	All	All	All
Hardware	Cisco	Catalyst 9800-40	-	All	All	All
Hardware	Cisco	Catalyst 9800-80	-	All	All	All
Hardware	Cisco	Catalyst 9800-cl	-	All	All	All
Hardware	Cisco	Catalyst 9800-I	-	All	All	All
Hardware	Cisco	Catalyst 9800-I-c	-	All	All	All
Hardware	Cisco	Catalyst 9800-I-f	-	All	All	All
Operating System	Cisco	Catalyst 9800 Firmware	17.3	All	All	All

Operating System	Cisco	Catalyst 9800 Firmware	17.5.1	All	All	All
Application	Cisco	Embedded Wireless Controller	All	All	All	All
Operating System	Cisco	ios Xe	17.3.1	All	All	All
Operating System	Cisco	ios Xe	17.3.2	All	All	All
Operating System	Cisco	ios Xe	17.4.1	All	All	All
Operating System	Cisco	ios Xe	17.5.1	All	All	All
Operating System	Cisco	ios Xe	3.15.1xbs	All	All	All
Operating System	Cisco	ios Xe	3.15.2xbs	All	All	All

References

Reference	Source	Link
Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Denial of Service Vulnerabilities	CISCO	tools.cisco.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[317049](#) Cisco Internetwork Operating System (IOS) XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Denial of Service (DoS) Vulnerability (cisco-sa-ewlc-capwap-dos-gmNjdKOY)

© 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