



CVE-2021-34770

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

Summary

CVE	CVE-2021-34770
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 03:36:00 UTC
Description	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE S

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst 9800	-	All	All	All
Hardware	Cisco	Catalyst 9800-40	-	All	All	All
Hardware	Cisco	Catalyst 9800-40 Wireless Controller	-	All	All	All
Hardware	Cisco	Catalyst 9800-80	-	All	All	All
Hardware	Cisco	Catalyst 9800-80 Wireless Controller	-	All	All	All
Hardware	Cisco	Catalyst 9800-cl	-	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-f	-	All	All	All
Hardware	Cisco	Catalyst 9800 Embedded Wireless Controller	-	All	All	All
Operating System	Cisco	ios Xe	All	All	All	All
Operating System	Cisco	ios Xe	16.10.1	All	All	All
Operating System	Cisco	ios Xe	16.10.1e	All	All	All
Operating System	Cisco	ios Xe	16.10.1s	All	All	All
Operating System	Cisco	ios Xe	16.11.1	All	All	All
Operating System	Cisco	ios Xe	16.11.1a	All	All	All
Operating System	Cisco	ios Xe	16.11.1b	All	All	All

Operating System	Cisco	ios Xe	16.11.1c	All	All	All
Operating System	Cisco	ios Xe	16.11.2	All	All	All
Operating System	Cisco	ios Xe	16.12.1	All	All	All
Operating System	Cisco	ios Xe	16.12.1s	All	All	All
Operating System	Cisco	ios Xe	16.12.1t	All	All	All
Operating System	Cisco	ios Xe	16.12.2s	All	All	All
Operating System	Cisco	ios Xe	16.12.2t	All	All	All
Operating System	Cisco	ios Xe	16.12.3	All	All	All
Operating System	Cisco	ios Xe	16.12.3s	All	All	All
Operating System	Cisco	ios Xe	16.12.4	All	All	All
Operating System	Cisco	ios Xe	16.12.4a	All	All	All
Operating System	Cisco	ios Xe	16.6.4s	All	All	All
Operating System	Cisco	ios Xe	17.1.1	All	All	All
Operating System	Cisco	ios Xe	17.1.1s	All	All	All
Operating System	Cisco	ios Xe	17.1.1t	All	All	All
Operating System	Cisco	ios Xe	17.1.2	All	All	All
Operating System	Cisco	ios Xe	17.1.3	All	All	All
Operating System	Cisco	ios Xe	17.2.1	All	All	All
Operating System	Cisco	ios Xe	17.2.1a	All	All	All
Operating System	Cisco	ios Xe	17.3.1	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 Remote Code Execution Vulnerability	CISCO	tools.cis
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317043 Cisco Internetwork Operating System (IOS) XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Remote Code Execution (RCE) Vulnerability (cisco-sa-ewlc-capwap-rce-LYgj8Kf)

© [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](#)