



CVE-2022-20682

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

Summary

CVE	CVE-2022-20682
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-15 15:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE V

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	16.11.1s	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	16.12.1a	All	All	All
Operating System	Cisco	ios Xe	16.12.1c	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	16.12.1w	All	All	All
Operating System	Cisco	ios Xe	16.12.1x	All	All	All
Operating System	Cisco	ios Xe	16.12.1y	All	All	All
Operating System	Cisco	ios Xe	16.12.1z	All	All	All
Operating System	Cisco	ios Xe	16.12.1z1	All	All	All
Operating System	Cisco	ios Xe	16.12.1z2	All	All	All

Operating System	Cisco	ios Xe	16.12.2	All	All	All
Operating System	Cisco	ios Xe	16.12.2a	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	16.12.3a	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	16.12.5	All	All	All
Operating System	Cisco	ios Xe	16.12.5a	All	All	All
Operating System	Cisco	ios Xe	16.12.5b	All	All	All
Operating System	Cisco	ios Xe	16.12.6	All	All	All
Operating System	Cisco	ios Xe	16.12.6a	All	All	All
Operating System	Cisco	ios Xe	17.1.1	All	All	All
Operating System	Cisco	ios Xe	17.1.1a	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	17.2.1r	All	All	All
Operating System	Cisco	ios Xe	17.2.1v	All	All	All
Operating System	Cisco	ios Xe	17.2.2	All	All	All
Operating System	Cisco	ios Xe	17.2.3	All	All	All
Operating System	Cisco	ios Xe	17.3.1	All	All	All
Operating System	Cisco	ios Xe	17.3.1a	All	All	All
Operating System	Cisco	ios Xe	17.3.1w	All	All	All
Operating System	Cisco	ios Xe	17.3.1x	All	All	All
Operating System	Cisco	ios Xe	17.3.1z	All	All	All
Operating System	Cisco	ios Xe	17.3.2	All	All	All
Operating System	Cisco	ios Xe	17.3.2a	All	All	All
Operating System	Cisco	ios Xe	17.3.3	All	All	All
Operating System	Cisco	ios Xe	17.3.3a	All	All	All

Operating System	Cisco	ios Xe	17.4.1	All	All	All
Operating System	Cisco	ios Xe	17.4.1a	All	All	All
Operating System	Cisco	ios Xe	17.4.1b	All	All	All
Operating System	Cisco	ios Xe	17.4.1c	All	All	All
Operating System	Cisco	ios Xe	17.4.2	All	All	All
Operating System	Cisco	ios Xe	17.4.2a	All	All	All
Operating System	Cisco	ios Xe	17.5.1	All	All	All
Operating System	Cisco	ios Xe	17.5.1a	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	Li
20220413 Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service Vulnerability	CISCO	to
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317147 Cisco Internetwork Operating System (IOS) XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service (DoS)Vulnerability (cisco-sa-c9800-capwap-mdns-6PSn7gKU)

© [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](#)