CVE-2020-3429

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-3429
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-24 18:15:00 UTC
Updated	2021-08-06 19:03:00 UTC
Description	A vulnerability in the WPA2 and WPA3 security implementation of Cisco IOS XE Wireless Controller Software for the Cisco

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst 9300	-	All	All	All
Hardware	Cisco	Catalyst 9300	-	All	All	All
Hardware	Cisco	Catalyst 9400	-	All	All	All
Hardware	Cisco	Catalyst 9400	-	All	All	All
Hardware	Cisco	Catalyst 9500	-	All	All	All
Hardware	Cisco	Catalyst 9500	-	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
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All

References

Reference	Source	Link
Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family WPA Denial of Service Vulnerability	CISCO	tools.cisco.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.