CVE-2017-12275

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

Summary

CVE	CVE-2017-12275
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-02 16:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the implementation of 802.11v Basic Service Set (BSS) Transition Management functionality in Cisco Wire

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wireless Lan Controller	-	All	All	All
Hardware	Cisco	Wireless Lan Controller	-	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	-	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	-	All	All	All

References

Reference
Cisco Wireless LAN Controller 802.11v Basic Service Set Transition Management Denial of Service Vulnerability
Cisco Wireless LAN Controller CVE-2017-12275 Denial of Service Vulnerability
Cisco Wireless LAN Controller 802.11v BSS Transition Management Response Packet Processing Flaw Lets Remote Users Cause the Targe
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report