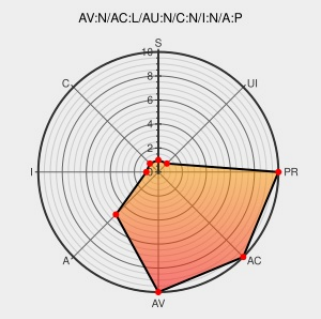
CVE-2013-6699

Published on: 11/22/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

CVE-2013-6699

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wireless Lan Controller from Cisco contain the following vulnerability:

The Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation on Cisco Wireless LAN Controller (WLC) devices allows remote attackers to cause a denial of service via a crafted CAPWAP packet that triggers a buffer over-read, aka Bug ID CSCuh81880.

CVE-2013-6699 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco Security Notice: Cisco Wireless LAN Controller Buffer Overread Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20131121 Cisco Wireless LAN Controller Buffer Overread Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wireless Lan Controller	All	All	All	All
Hardware	Cisco	Wireless Lan Controller	All	All	All	All

cpe:2.3:h:cisco:wireless_lan_controller:*:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:wireless_lan_controller:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→