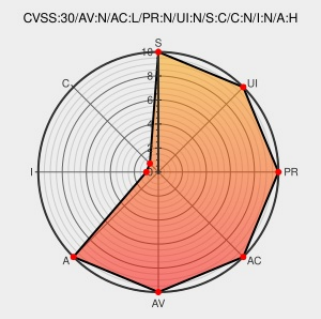
CVE-2020-3492

Published on: 09/24/2020 12:00:00 AM UTC

Last Modified on: 10/19/2021 06:44:00 PM UTC

CVE-2020-3492 - advisory for cisco-sa-iosxe-wlc-fnfv9-EvrAQpNX

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



Certain versions of Catalyst 9800-40 from Cisco contain the following vulnerability:

A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Software for Cisco Wireless LAN Controllers (WLC) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of certain parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by spoofing the address of an existing Access Point on the network and sending a Control and Provisioning of Wireless Access Points (CAPWAP) packet that includes a crafted Flexible NetFlow Version 9 record to an affected device. A successful exploit could allow the attacker to cause a process crash that would lead to a reload of the device.

CVE-2020-3492 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Wireless LAN Controller (WLC)** version **n/a**

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco IOS XE Software for Catalyst 9800 Series and Cisco AireOS Software for Cisco WLC Flexible NetFlow Version 9 Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200924 Cisco IOS XE Software for Catalyst 9800 Series and Cisco AireOS Software for Cisco WLC Flexible NetFlow Version 9 Denial of Service 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	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
Hardware	Cisco	Catalyst 9800-l-c	-	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-l-f	-	All	All	All
Operating System	Cisco	Ios Xe	16.12.1	All	All	All
Operating System	Cisco	Ios Xe	16.12.1	All	All	All

cpe:2.3:h:cisco:catalyst_9800-40:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-40:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-80:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-80:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-cl:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-cl:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l-c:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l-c:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l-f:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:catalyst_9800-l-f:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→