

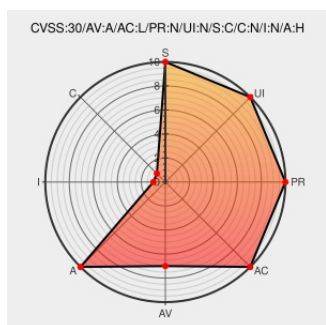


CVE-2020-3488

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

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

CVE-2020-3488 - advisory for cisco-sa-capwap-dos-TPdNTdyq

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Catalyst 9800-40](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition of an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit these vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition on the affected device.

CVE-2020-3488 has been assigned by [Cisco](#) 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 vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco IOS XE Software** version n/a

CVSS3 Score: **7.4 - HIGH**

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

CVSS2 Score: **6.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact

Impact

Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service Vulnerabilities

Vendor Advisory

tools.cisco.com

text/html

 CISCO 20200924 Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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→

© CVE.report 2023 |

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