



CVE-2020-3399

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

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3399 - advisory for cisco-sa-capwap-dos-ShFzXf

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H



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

A vulnerability 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, remote attacker to cause a denial of service (DoS) condition of an affected device. The vulnerability is due to insufficient

input validation during CAPWAP packet processing. An attacker could exploit this vulnerability by sending a crafted CAPWAP packet to an affected device, resulting in a buffer over-read. 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-2020-3399 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 vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco IOS XE Software** 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	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 Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20200924 Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service Vulnerability				
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	All	All	All
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All
Operating System	Cisco	Ios Xe	16.12.2	All	All	All
Operating System	Cisco	Ios Xe	16.12	All	All	All
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All

Operating System	Cisco	ios Xe	16.12.2	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:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios_xe:16.12.1s:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios_xe:16.12.2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios_xe:16.12:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios_xe:16.12.1s:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios_xe:16.12.2:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)