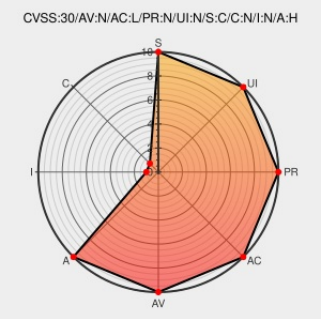
# CVE-2020-3221

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 09/17/2021 06:41:00 PM UTC

## CVE-2020-3221 - advisory for cisco-sa-iosxe-fnfv9-dos-HND6Fc9u

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 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device.

CVE-2020-3221 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 IOS XE Software 16.10.1** 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 Software Flexible NetFlow Version 9 Denial of Service Vulnerability | Patch<br>Vendor Advisory<br>tools.cisco.com<br>text/html | CISCO 20200603 Cisco IOS XE Software 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 | 16.10.1 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1b | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1e | All | All | All |
| Operating | Cisco | Ios Xe | 16.10.1s | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| System | | | | | | |
| Operating System | Cisco | Ios Xe | 16.10.2 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1b | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1c | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1s | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1c | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1s | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1t | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1b | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1e | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.1s | All | All | All |
| Operating System | Cisco | Ios Xe | 16.10.2 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1 | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1b | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1c | All | All | All |
| Operating System | Cisco | Ios Xe | 16.11.1s | All | All | All |
| Operating | Cisco | Ios Xe | 16.12.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| System | | | | | | |
| Operating System | Cisco | Ios Xe | 16.12.1a | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1c | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1s | All | All | All |
| Operating System | Cisco | Ios Xe | 16.12.1t | 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:16.10.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1s:*:*:*:*:*:*:*:

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

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

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

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

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

cpe:2.3:o:cisco:ios_xe:16.10.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1s:*:*:*:*:*:*:*:

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

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

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

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

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

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|

← Previous ID

Next ID→

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