



# CVE-2023-20233

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-20233
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-13 17:15:00 UTC
<b>Updated</b>	2024-01-25 17:15:00 UTC
<b>Description</b>	A vulnerability in the Connectivity Fault Management (CFM) feature of Cisco IOS XR Software could allow an unauthenticated

## Risk And Classification

**Problem Types:** CWE-354

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xr	All	All	All	All
Operating System	Cisco	ios Xr	7.9.0	All	All	All

## References

Reference	Source	Link	Tags
Cisco IOS XR Software Connectivity Fault Management Denial of Service Vulnerability	MISC	<a href="https://sec.cloudapps.cisco.com">sec.cloudapps.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, c

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[317358](#) Cisco Internetwork Operating System (IOS) XR Software Denial of Service (DoS) Vulnerability (cisco-sa-ios-xr-cfm-3pWN8MKt)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)