



CVE-2018-0132

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

Summary

CVE	CVE-2018-0132
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-08 07:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the forwarding information base (FIB) code of Cisco IOS XR Software could allow an unauthenticated, remote user to cause a denial of service (DoS) condition on the affected device by sending a specially crafted packet to the affected device.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Carrier Routing System	5.3.0.rout	All	All	All
Application	Cisco	Carrier Routing System	5.3.0.rout	All	All	All

References

Reference	Source	Link	Tags
Malformed Request	BID	www.securityfocus.com	This
Cisco IOS XR Software Routing and Forwarding Inconsistency Denial of Service Vulnerability	CONFIRM	tools.cisco.com	Ver
Cisco IOS XR Routing Update Bug Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	This
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)