

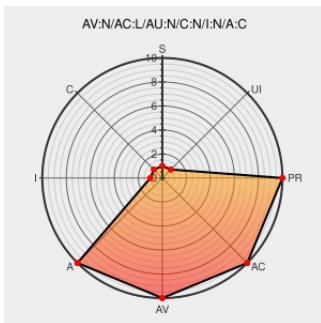


CVE-2011-1651

Published on: 05/31/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1651

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

Certain versions of **ios Xr** from **Cisco** contain the following vulnerability: Cisco IOS XR 3.9.x and 4.0.x before 4.0.3 and 4.1.x before 4.1.1, when an SPA interface processor is installed, allows remote attackers to cause a denial of service (device reload) via a crafted IPv4 packet, aka Bug ID CSCto45095.

CVE-2011-1651 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

COMPLETE

CVE References

Description

Tags

Link

Cisco Security Advisory: Cisco XR 12000 Series Shared Port Adapters Interface Processor Vulnerability - Cisco Systems

[Vendor Advisory](#)
www.cisco.com
[text/html](#)

[CISCO 20110525 Cisco XR 12000 Series Shared Port Adapters Interface Processor Vulnerability](#)

Cisco IOS XR SPA Interface Processor IPv4 Packet Processing Flaw Lets Remote Users Deny Service - SecurityTracker

www.securitytracker.com
[text/html](#)

[SECTRAK 1025567](#)

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
Operating System	Cisco	ios Xr	3.0	All	All	All
Operating System	Cisco	ios Xr	3.9.0	All	All	All
Operating System	Cisco	ios Xr	3.9.1	All	All	All
Operating System	Cisco	ios Xr	3.9.2	All	All	All
Operating System	Cisco	ios Xr	4.0.0	All	All	All
Operating System	Cisco	ios Xr	4.0.1	All	All	All
Operating System	Cisco	ios Xr	4.0.2	All	All	All
Operating System	Cisco	ios Xr	4.1	All	All	All
Operating System	Cisco	ios Xr	3.0	All	All	All
Operating System	Cisco	ios Xr	3.9.0	All	All	All
Operating System	Cisco	ios Xr	3.9.1	All	All	All
Operating System	Cisco	ios Xr	3.9.2	All	All	All
Operating System	Cisco	ios Xr	4.0.0	All	All	All
Operating System	Cisco	ios Xr	4.0.1	All	All	All
Operating System	Cisco	ios Xr	4.0.2	All	All	All
Operating System	Cisco	ios Xr	4.1	All	All	All
cpe:2.3:o:cisco:ios_xr:3.0:*****:						
cpe:2.3:o:cisco:ios_xr:3.9.0:*****:						
cpe:2.3:o:cisco:ios_xr:3.9.1:*****:						
cpe:2.3:o:cisco:ios_xr:3.9.2:*****:						
cpe:2.3:o:cisco:ios_xr:4.0.0:*****:						
cpe:2.3:o:cisco:ios_xr:4.0.1:*****:						
cpe:2.3:o:cisco:ios_xr:4.0.2:*****:						

cpe:2.3:o:cisco:ios_xr:4.1:*****:
cpe:2.3:o:cisco:ios_xr:3.0:*****:
cpe:2.3:o:cisco:ios_xr:3.9.0:*****:
cpe:2.3:o:cisco:ios_xr:3.9.1:*****:
cpe:2.3:o:cisco:ios_xr:3.9.2:*****:
cpe:2.3:o:cisco:ios_xr:4.0.0:*****:
cpe:2.3:o:cisco:ios_xr:4.0.1:*****:
cpe:2.3:o:cisco:ios_xr:4.0.2:*****:
cpe:2.3:o:cisco:ios_xr:4.1:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →