CVE-2014-8014

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-8014
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-18 16:59:16 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco IOS XR allows remote attackers to cause a denial of service (RSVP process reload) via a malformed RSVP packet, a

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-19 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Lin
Cisco IOS XR RSVP Processing Flaw Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108	ww
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-8014	af854a3a-2127-422b-91ae-364da2661108	tool
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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