



CVE-2013-1234

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

Summary

CVE	CVE-2013-1234
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-03 11:57:44 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SNMP module in Cisco IOS XR allows remote authenticated users to cause a denial of service (process restart) via cra

Risk And Classification

Primary CVSS: v2.0 4 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:S/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		Link	
Cisco IOS XR Software Crafted SNMP Packets Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108		tools.cisco.com	
CVE Program record	CVE.ORG		www.cve.org	
NVD vulnerability detail	NVD		nvd.nist.gov	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				