



CVE-2016-1407

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

Summary	
CVE	CVE-2016-1407
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-25 01:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco IOS XR through 5.3.2 mishandles Local Packet Transport Services (LPTS) flow-base entries, which allows remote at

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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
Hardware	Cisco	Asr 9001	-	All	All	All
Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9010	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All
Operating System	Cisco	Ios Xr	2.0.0	All	All	All
Operating System	Cisco	Ios Xr	3.0.0	All	All	All
Operating System	Cisco	Ios Xr	3.0.1	All	All	All
Operating System	Cisco	Ios Xr	3.2.0	All	All	All
Operating System	Cisco	Ios Xr	3.2.1	All	All	All
Operating System	Cisco	Ios Xr	3.2.2	All	All	All
Operating System	Cisco	Ios Xr	3.2.3	All	All	All
Operating System	Cisco	Ios Xr	3.2.4	All	All	All
Operating System	Cisco	Ios Xr	3.2.50	All	All	All
Operating System	Cisco	Ios Xr	3.2.6	All	All	All
Operating System	Cisco	Ios Xr	3.3.0	All	All	All

Operating System	Cisco	ios Xr	3.3.1	All	All	All
Operating System	Cisco	ios Xr	3.3.2	All	All	All
Operating System	Cisco	ios Xr	3.3.3	All	All	All
Operating System	Cisco	ios Xr	3.3.4	All	All	All
Operating System	Cisco	ios Xr	3.4.0	All	All	All
Operating System	Cisco	ios Xr	3.4.1	All	All	All
Operating System	Cisco	ios Xr	3.4.2	All	All	All
Operating System	Cisco	ios Xr	3.4.3	All	All	All
Operating System	Cisco	ios Xr	3.5.0	All	All	All
Operating System	Cisco	ios Xr	3.5.2	All	All	All
Operating System	Cisco	ios Xr	3.5.3	All	All	All
Operating System	Cisco	ios Xr	3.5.4	All	All	All
Operating System	Cisco	ios Xr	3.6.0	All	All	All
Operating System	Cisco	ios Xr	3.6.1	All	All	All
Operating System	Cisco	ios Xr	3.6.2	All	All	All
Operating System	Cisco	ios Xr	3.6.3	All	All	All
Operating System	Cisco	ios Xr	3.6_base	All	All	All
Operating System	Cisco	ios Xr	3.7.0	All	All	All
Operating System	Cisco	ios Xr	3.7.1	All	All	All
Operating System	Cisco	ios Xr	3.7.2	All	All	All
Operating System	Cisco	ios Xr	3.7.3	All	All	All
Operating System	Cisco	ios Xr	3.7_base	All	All	All
Operating System	Cisco	ios Xr	3.8.0	All	All	All
Operating System	Cisco	ios Xr	3.8.1	All	All	All
Operating System	Cisco	ios Xr	3.8.2	All	All	All
Operating System	Cisco	ios Xr	3.8.3	All	All	All
Operating System	Cisco	ios Xr	3.8.4	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	3.9.3	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	4.0.11	All	All	All
Operating System	Cisco	ios Xr	4.0.2	All	All	All
Operating System	Cisco	ios Xr	4.0.3	All	All	All

Operating System	Cisco	ios Xr	4.0.3	All	All	All
Operating System	Cisco	ios Xr	4.0.4	All	All	All
Operating System	Cisco	ios Xr	4.0_base	All	All	All
Operating System	Cisco	ios Xr	4.1.0	All	All	All
Operating System	Cisco	ios Xr	4.1.1	All	All	All
Operating System	Cisco	ios Xr	4.1.2	All	All	All
Operating System	Cisco	ios Xr	4.1_base	All	All	All
Operating System	Cisco	ios Xr	4.2.0	All	All	All
Operating System	Cisco	ios Xr	4.2.1	All	All	All
Operating System	Cisco	ios Xr	4.2.2	All	All	All
Operating System	Cisco	ios Xr	4.2.3	All	All	All
Operating System	Cisco	ios Xr	4.2.4	All	All	All
Operating System	Cisco	ios Xr	4.3.0	All	All	All
Operating System	Cisco	ios Xr	4.3.1	All	All	All
Operating System	Cisco	ios Xr	4.3.2	All	All	All
Operating System	Cisco	ios Xr	4.3.3	All	All	All
Operating System	Cisco	ios Xr	4.3.4	All	All	All
Operating System	Cisco	ios Xr	5.0.0	All	All	All
Operating System	Cisco	ios Xr	5.0.1	All	All	All
Operating System	Cisco	ios Xr	5.0_base	All	All	All
Operating System	Cisco	ios Xr	5.1.0	All	All	All
Operating System	Cisco	ios Xr	5.1.1.k9sec	All	All	All
Operating System	Cisco	ios Xr	5.1.2	All	All	All
Operating System	Cisco	ios Xr	5.1.3	All	All	All
Operating System	Cisco	ios Xr	5.2.0	All	All	All
Operating System	Cisco	ios Xr	5.2.1	All	All	All
Operating System	Cisco	ios Xr	5.2.2	All	All	All
Operating System	Cisco	ios Xr	5.2.3	All	All	All
Operating System	Cisco	ios Xr	5.2.4	All	All	All
Operating System	Cisco	ios Xr	5.2.5	All	All	All
Operating System	Cisco	ios Xr	5.3.0	All	All	All
Operating System	Cisco	ios Xr	5.3.1	All	All	All
Operating System	Cisco	ios Xr	5.3.2	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		

CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
Cisco ASR 9000 Series Router LPTS Flow Handling Flaw Lets Remote Users Consume Excessive Resources on the Target System - Security				
Cisco IOS XR Software LPTS Denial of Service Vulnerability				
CVE Program record				
NVD vulnerability detail				
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)