



CVE-2017-12236

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

Summary

CVE	CVE-2017-12236
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-29 01:34:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the implementation of the Locator/ID Separation Protocol (LISP) in Cisco IOS XE 3.2 through 16.5 could a

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xe	16.5.1c	All	All	All
Operating System	Cisco	ios Xe	3.2.0ja	All	All	All
Operating System	Cisco	ios Xe	3.9.1e	All	All	All
Operating System	Cisco	ios Xe	16.5.1c	All	All	All
Operating System	Cisco	ios Xe	3.2.0ja	All	All	All
Operating System	Cisco	ios Xe	3.9.1e	All	All	All

References

Reference	Source
Cisco IOS XE LISP Protocol Bug Lets Remote Users Bypass Authentication on the Map Server/Map Resolver - SecurityTracker	SECTRACI
Cisco IOS XE Software Locator/ID Separation Protocol Authentication Bypass Vulnerability	CONFIRM
Malformed Request	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)