



CVE-2017-12272

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

Summary

CVE	CVE-2017-12272
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-19 08:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the web framework code of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cor

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xe	16.1.2	All	All	All
Operating System	Cisco	ios Xe	16.2.0	All	All	All
Operating System	Cisco	ios Xe	16.3(1)	All	All	All
Operating System	Cisco	ios Xe	16.3\1\	All	All	All
Operating System	Cisco	ios Xe	16.1.2	All	All	All
Operating System	Cisco	ios Xe	16.2.0	All	All	All
Operating System	Cisco	ios Xe	16.3\1\	All	All	All

References

Reference	Source
Cisco IOS XE Input Validation Flaw in Web Framework Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTR
Cisco IOS XE Software Web Framework Cross-Site Scripting Vulnerability	CONFIF
Cisco IOS XE Software CVE-2017-12272 Cross Site Scripting Vulnerability	BID
CVE Program record	CVE.OP
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](#)