



CVE-2017-12230

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

Summary

CVE	CVE-2017-12230
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 web-based user interface (web UI) of Cisco IOS XE 16.2 could allow an authenticated, remote attacker

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	16.2.1	All	All	All
Operating System	Cisco	Ios Xe	16.2.1	All	All	All

References

Reference
Malformed Request
Cisco IOS XE Web User Interface Default Permissions Error Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker
Cisco IOS XE Software Web UI Privilege Escalation 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.

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