



CVE-2018-0152

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

Summary

CVE	CVE-2018-0152
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-28 22:29:00 UTC
Updated	2019-12-03 18:54:00 UTC
Description	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote att

Risk And Classification

Problem Types: CWE-613

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	16.1.1	All	All	All
Operating System	Cisco	Ios Xe	16.1.1	All	All	All

References

Reference	Source
Cisco IOS XE Web Interface Access Control Bug Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTRAK
Cisco IOS XE Software Web UI Remote Access Privilege Escalation Vulnerability	CONFIRM
Cisco IOS XE Software CVE-2018-0152 Remote Privilege Escalation Vulnerability	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.

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