



CVE-2019-1881

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

Summary

CVE	CVE-2019-1881
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-05 17:29:00 UTC
Updated	2019-10-09 23:48:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Industrial Network Director (IND) could allow an unauthenticated user to perform a cross-site request forgery (CSRF) attack and change the configuration of the device. This vulnerability is present in versions 1.5(0.250) and earlier.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Industrial Network Director	1.5(0.250)	All	All	All
Application	Cisco	Industrial Network Director	1.5\ (0.250\)	All	All	All
Application	Cisco	Industrial Network Director	1.5\ (0.250\)	All	All	All

References

Reference	Source	Link	Tags
Cisco Industrial Network Director Cross-Site Request Forgery Vulnerability	CISCO	tools.cisco.com	Vendor /
Cisco Industrial Network Director CVE-2019-1881 Cross Site Request Forgery Vulnerability	BID	www.securityfocus.com	Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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