



CVE-2019-1861

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

Summary

CVE	CVE-2019-1861
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-05 17:29:00 UTC
Updated	2020-10-16 15:42:00 UTC
Description	A vulnerability in the software update feature of Cisco Industrial Network Director could allow an authenticated, remote attacker to execute arbitrary code on the affected device.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Industrial Network Director	All	All	All	All
Application	Cisco	Industrial Network Director	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Industrial Network Director CVE-2019-1861 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party
Cisco Industrial Network Director Remote Code Execution Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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