CVE-2020-3531

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-3531
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-18 19:15:00 UTC
Updated	2020-12-02 15:30:00 UTC
Description	A vulnerability in the REST API of Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Cisco IoT Field Network Director Unauthenticated REST API Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report