



CVE-2019-12115

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

Summary

CVE	CVE-2019-12115
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-18 19:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	An issue was discovered in ONAP SDC through Dublin. By accessing port 4000 of demo-sdc-sdc-be pod, an unauthenticated user can execute arbitrary code on the host. The issue is caused by a missing authentication check in the SDC through Dublin API. The issue affects versions 1.1.0 through 1.1.1. The issue is fixed in version 1.1.2.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Onap	Open Network Automation Platform	All	All	All	All
Application	Onap	Open Network Automation Platform	All	All	All	All

References

Reference	Source	Link
[OJSI-10] Some ONAP services exposes JDWP outside of pod which allows for arbitrary code execution - ONAP	MISC	jira.onap.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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