CVE-2019-20329

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-20329
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-03 00:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	OpenLambda 2019-09-10 allows DNS rebinding attacks against the OL server for the REST API on TCP port 5000.

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openlambda Project	Openlambda	2019-09-10	All	All	All
Application	Openlambda Project	Openlambda	2019-09-10	All	All	All

References

Reference	Source	Link
OL-Server vulnerable to DNS Rebinding attacks. · Issue #92 · open-lambda/open-lambda · GitHub	MISC	github
open-lambda/config.go at 9f7f935195ca74700c60ebc1ecfdaefad40d144b · open-lambda/open-lambda · GitHub	MISC	github
open-lambda/lambdaServer.go at 9f7f935195ca74700c60ebc1ecfdaefad40d144b · open-lambda/open-lambda · GitHub	MISC	github
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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