CVE-2020-11091

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

Summary

CVE	CVE-2020-11091
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-03 23:15:00 UTC
Updated	2020-06-09 20:02:00 UTC
Description	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS reque

Risk And Classification

Problem Types: CWE-350

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Weave	Weave Net	All	All	All	All
Application	Weave	Weave Net	All	All	All	All

References

Reference	Source	L
IPv4 only clusters susceptible to MitM attacks via IPv6 rogue router advertisements · Advisory · weaveworks/weave · GitHub	CONFIRM	g
Merge pull request #3801 from weaveworks/disable-accept-ra · weaveworks/weave@15f21f1 · GitHub	MISC	g
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982384 Go (go) Security Update for github.com/weaveworks/weave (GHSA-59qg-grp7-5r73)

Free CVE JSON API cve.report/api

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