



CVE-2020-26278

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

Summary

CVE	CVE-2020-26278
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-20 22:15:00 UTC
Updated	2021-02-02 15:26:00 UTC
Description	Weave Net is open source software which creates a virtual network that connects Docker containers across multiple hosts

Risk And Classification

Problem Types: CWE-250

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
weave/CHANGELOG.md at master · weaveworks/weave · GitHub	MISC	github.com
Stop running in host PID namespace · weaveworks/weave@a0ac81b · GitHub	MISC	github.com
Weave Net Pods can be used to escalate other Kubernetes vulnerabilities · Advisory · weaveworks/weave · GitHub	CONFIRM	github.com
For K8s, stop running in host PID namespace by bboreham · Pull Request #3876 · weaveworks/weave · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)