



CVE-2019-3779

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-3779
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-08 16:29:00 UTC
Updated	2019-10-09 23:49:00 UTC
Description	Cloud Foundry Container Runtime, versions prior to 0.29.0, deploys Kubernetes clusters utilize the same CA (Certificate Au

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudfoundry	Container Runtime	All	All	All	All
Application	Cloudfoundry	Container Runtime	All	All	All	All

References

Reference	Source
CVE-2019-3779: Cloud Foundry Container Runtime allows a user to bypass security policy when talking to ETCD Cloud Foundry	CONFIR
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)