



CVE-2019-3784

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

Summary

CVE	CVE-2019-3784
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-07 18:29:00 UTC
Updated	2019-10-09 23:49:00 UTC
Description	Cloud Foundry Stratos, versions prior to 2.3.0, contains an insecure session that can be spoofed. When deployed on cloud

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudfoundry	Stratos	All	All	All	All
Application	Cloudfoundry	Stratos	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2019-3784: Stratos contains a Session Collision Vulnerability Cloud Foundry	CONFIRM	www.cloudfoundry.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)