



# CVE-2020-5409

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

## Summary

<b>CVE</b>	CVE-2020-5409
<b>State</b>	PUBLIC
<b>Assigner</b>	security@pivotal.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-14 00:15:00 UTC
<b>Updated</b>	2020-05-15 13:43:00 UTC
<b>Description</b>	Pivotal Concourse, most versions prior to 6.0.0, allows redirects to untrusted websites in its login flow. A remote unauthenti

## Risk And Classification

**Problem Types:** CWE-601

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Pivotal Software</a>	<a href="#">Concourse</a>	All	All	All	All
Application	<a href="#">Pivotal Software</a>	<a href="#">Concourse</a>	All	All	All	All

## References

Reference	Source	Link	Tags
CVE-2020-5409: Concourse Open Redirect in the /sky/login endpoint   Security   VMware Tanzu	CONFIRM	<a href="https://tanzu.vmware.com">tanzu.vmware.com</a>	Vendor
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#)**