



CVE-2022-23726

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

Summary

CVE	CVE-2022-23726
State	PUBLIC
Assigner	responsible-disclosure@pingidentity.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-30 15:15:00 UTC
Updated	2022-10-04 16:33:00 UTC
Description	PingCentral versions prior to listed versions expose Spring Boot actuator endpoints that with administrative authentication r

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pingidentity	Pingcentral	All	All	All	All

References

Reference	Source	Link	Tags
Ping Identity Documentation Portal	CONFIRM	docs.pingidentity.com	
Download PingCentral Ping Identity	MISC	www.pingidentity.com	
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](#)