



CVE-2023-39231

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-39231
State	PUBLIC
Assigner	responsible-disclosure@pingidentity.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-10-31 18:47:00 UTC
Description	PingFederate using the PingOne MFA adapter allows a new MFA device to be paired without requiring second factor authentication

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pingidentity	Pingone Mfa Integration Kit	2.2	All	All	All

References

Reference	Source	Link
PingID Downloads	MISC	www.pingidentity.com
Release Notes - PingOne - PingFederate - PingOne MFA - PingOne Cloud Platform - PingOne Services	MISC	docs.pingidentity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report