Insufficient granularity of access control for Remote Connector Servers in client mode

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-20628
State	PUBLISHED
Assigner	Ping Identity
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 23:16:27 UTC
Updated	2026-04-08 21:26:35 UTC
Description	An insufficient granularity of access control vulnerability exists in PingIDM (formerly ForgeRock Identity Management) wher

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from responsible-disclosure@pingidentity.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:P/AU:Y/R:U/V:C/RE:M/U:Red

EPSS: 0.000540000 probability, percentile 0.167690000 (date 2026-04-14)

Problem Types: CWE-1220 | CWE-1220 CWE-1220 Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
4.0	responsible-disclosure@pingidentity.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:I
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:I

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:P/AU:Y/R:U/V:C/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ping Identity	PingIDM	affected 7.5.0 custom	Not specified
CNA	Ping Identity	PingIDM	affected 7.4.0 7.4.1 custom	Not specified
CNA	Ping Identity	PingIDM	affected 7.3.0 7.3.1 custom	Not specified
CNA	Ping Identity	PingIDM	affected 7.2.0 7.2.2 custom	Not specified
CNA	Ping Identity	PingIDM	affected 7.1.* custom	Not specified

References

Reference	Source	Link
backstage.pingidentity.com/downloads/browse/idm/featured	responsible-disclosure@pingidentity.com	backstage.pingidentity.com
backstage.forgerock.com/knowledge/advisories/article/a14305629	responsible-disclosure@pingidentity.com	backstage.forgerock.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.

Additional Advisory Data

Solutions

CNA: Both of the following steps are required to mitigate the issue: * Upgrade to one of the fixed versions listed previously. * Secure the /openicf endpoint using the new access and

authentication configuration options (refer to migration dependent features https://docs.pingidentity.com/pingoneaic/latest/product-information/migration-dependent-features.html#current_migration_dependent_features for more details).

Workarounds

CNA: Configure a reverse proxy (such as PingGateway) to enforce IP and certificate-based rules to the /openicf endpoint.

CNA: Configure all RCS instances to run in server mode.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**