



CVE-2026-8654

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-8654 |
| State | PUBLISHED |
| Assigner | Perforce |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-15 07:16:20 UTC |
| Updated | 2026-05-15 07:16:20 UTC |
| Description | Improper input validation in Delphix Continuous Data connectors allows an authenticated user to execute arbitrary operating |

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from security@puppet.com

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

Problem Types: CWE-78 | CWE-78 CWE-78 Improper neutralization of special elements used in an OS command ('OS command injection')

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|-----------|-------|----------|--|
| 4.0 | security@puppet.com | Secondary | 8.7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0 | CNA | CVSS | 8.7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---|---|--------------------------|---------------|
| CNA | Delphix Continuous Data | IBM Db2 Connector | affected 2025.2 custom | Not specified |
| CNA | Delphix Continuous Data | MangoDB Connector | affected 2025.2.1 custom | Not specified |
| CNA | Delphix Continuous Data | PostgreSQL Connector | affected 2025.1.0 custom | Not specified |
| CNA | Delphix Continuous Data | MySQL Connector | affected 2025.1.0 custom | Not specified |
| CNA | Delphix Continuous Data | Oracle EBS Connector | affected 2025.2.0 custom | Not specified |
| CNA | Delphix Continuous Data | SAP HANA Connector | affected 2026.2.0 custom | Not specified |
| CNA | Delphix Continuous Data | CockroachDB Connector | affected 2025.2.0 custom | Not specified |
| CNA | Delphix Continuous Data | Couchbase Connector | affected 1.3.2 semver | Not specified |
| CNA | Delphix Continuous Data | Cassandra Connector | affected 2025.1.0 custom | Not specified |
| CNA | Delphix Continuous Data | YugabyteDB Connector | affected 2025.1.1 custom | Not specified |
| CNA | Delphix Continuous Data | MSSQL On Linux Connector | affected 2025.1.0 custom | Not specified |
| CNA | Delphix Continuous Data | Oracle Backup Ingestion Connector | affected 4.2.1 semver | Not specified |

References

| Reference | Source | Link | Tag |
|---|--|---|-----|
| portal.perforce.com/s/cve/a91Qi000002z78HIAQ/authenticated-os-command-injection-i... | security@puppet.com | portal.perforce.com | |
| CVE Program record | CVE.ORG | www.cve.org | can |
| NVD vulnerability detail | NVD | nvd.nist.gov | can |

No vendor comments have been submitted for this CVE.

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 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](#)