



# Code Injection in Perforce P4 (Helix Core)

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

## Summary

<b>CVE</b>	CVE-2026-6902
<b>State</b>	PUBLISHED
<b>Assigner</b>	Perforce
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-18 09:16:24 UTC
<b>Updated</b>	2026-05-18 20:27:12 UTC
<b>Description</b>	A vulnerability in Command-Line Client in P4 Server prior to the 2025.2 Patch 2, identified as CVE-2026-6902, has been fix

## Risk And Classification

**Primary CVSS:** v4.0 7.7 HIGH from security@puppet.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/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-94 | CWE-94 CWE-94 Code Injection

Version	Source	Type	Score	Severity	Vector
4.0	security@puppet.com	Secondary	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:X
4.0	CNA	CVSS	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/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	Perforce	P4 Helix Core	affected P4 (Helix Core) 2025.2 Patch 2 custom	Not specified

### References

Reference	Source	Link	Tags
portal.perforce.com/s/cve/a91Qi000002zJB3IAM/code-injection-in-perforce-helix-core	security@puppet.com	portal.perforce.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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