CISA Adds Critical Perforce Puppet Flaw CVE-2026-115731 to Exploited Vulnerabilities List



CISA has added a critical flaw in Perforce Puppet, tracked as CVE-2026-115731 (CVSS 9.4), to its KEV catalog after reports of active exploitation. Organisations running Puppet should check their exposure.

- CISA added the Perforce Puppet vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on Tuesday.
- The flaw is tracked as CVE-2026-115731 and carries a CVSS score of 9.4.
- CISA cited reports of active exploitation.
- Puppet is an enterprise infrastructure-as-code and configuration management platform.
- The source excerpt is truncated and does not describe the exact flaw type, affected versions or fixes.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability in Perforce Puppet to its Known Exploited Vulnerabilities (KEV) catalog, saying it has seen reports of active exploitation.

What is known

The flaw is tracked as **CVE-2026-115731** and has a CVSS score of 9.4. Puppet is an enterprise platform for infrastructure-as-code and configuration management. The headline of the original report describes the issue as a remote code execution flaw affecting enterprise management servers.

The excerpt we reviewed is cut off. It does not state the technical root cause, the affected versions, the attackers involved, or whether a patch is available. We have therefore not included those details.

Why it matters

Configuration management servers typically hold wide administrative reach over the systems they manage. A critical flaw that is already being exploited in such a platform deserves prompt attention, particularly in regulated environments where change control and privileged access are closely supervised.

Recommended approach

Institutions should first confirm whether Puppet is used anywhere in their estate, including by subsidiaries and service providers. If it is, consult the vendor's advisory for affected versions and fixes, and prioritise remediation in line with your vulnerability management process. Until then, limit network access to Puppet servers and review them for unusual activity.

What to do now

1. Inventory all Puppet servers and agents, including those run by subsidiaries and third parties.
2. Review the Perforce advisory for CVE-2026-115731 to identify affected versions and available fixes.
3. Patch or apply vendor mitigations on an emergency basis, starting with internet-reachable or high-privilege servers.
4. Restrict network access to Puppet servers to approved management networks only.
5. Review logs and configuration changes on Puppet servers for unexpected activity and escalate any findings through incident response.