GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

18 November 2026

Advisory 379: Perforce Puppet Enterprise and OpenVox Deserialization of Untrusted Data Vulnerability (CVE-2026-115731).

Release Date: 7th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-115731 is a critical deserialization of untrusted data vulnerability (CWE-502 and CWE-94) in the report-processing code of Puppet Server, the central server of the Puppet and OpenVox configuration management platforms. Perforce rates it CVSS v4.0 9.4. Any client holding a CA-signed agent certificate can submit a report containing a crafted rich-data type and run arbitrary code on the Puppet Server as its service user.

What are the systems affected?

The vulnerability affects Puppet Server in all known Puppet and OpenVox implementations, including:

- Puppet Enterprise 2023.8.0 before 2023.8.13
- Puppet Enterprise 2025.0.0 before 2025.12.1
- Puppet Enterprise 2026.0.0 before 2026.0.1
- OpenVox Server before 9.2.0 and 8.18.0, OpenVox Agent before 9.3.0 and 8.32.0, and OpenVoxDB before 9.2.0 and 8.18.0

- Open-source Puppet and puppetserver packages, and products that bundle them, such as Red Hat Satellite clients and Linux distribution packages
- Servers with certificate autosigning enabled are at the highest risk

Not affected / patched version:

- Puppet Enterprise 2023.8.13, 2025.12.1 or 2026.0.1 or later
- OpenVox Server 9.2.0 or 8.18.0, OpenVox Agent 9.3.0 or 8.32.0, and OpenVoxDB 9.2.0 or 8.18.0 or later
- Patched distribution packages, for example Debian DSA-6608-1 and DLA-4884-1 and Red Hat Satellite client updates

What does this mean?

Successful exploitation may allow attackers to:

- Run code on the Puppet Server as its service user
- Steal the Puppet certificate authority signing key and issue trusted certificates
- Push malicious configuration or code to every machine managed by the server
- Read secrets, passwords and keys stored in Puppet code and data
- Use the server as a foothold for wider network compromise

Mitigation process

CERTVU recommends the following:

1. Update Puppet Server, agents and PuppetDB
Upgrade Puppet Enterprise to 2023.8.13, 2025.12.1 or 2026.0.1, or OpenVox to the fixed server, agent and database versions listed above. Apply vendor updates for distribution packages and bundled products. Update every component, including compilers, agents and any repackaged copies.

2. Disable or tighten certificate autosigning
3. Restrict access to Puppet Server
4. Check for compromise

Report incidents to CERTVU at incident@cert.gov.vu.

1. https://www.cve.org/CVERecord?id=CVE-2026-115731
2. https://github.com/OpenVoxProject/openvox/security/advisories/GHSA-ffr6-rwpm-p5wq
3. https://voxpupuli.org/blog/2026/11/03/critical-cve-updates/
4. https://www.cisa.gov/news-events/alerts/2026/11/17/cisa-adds-one-known-exploited-vulnerability-catalog
5. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-115731