

Puppet Core CVE Remediation Summary

Perforce Puppet is committed to remediating critical and high-severity vulnerabilities affecting Puppet software and 3rd-party libraries within the guaranteed SLA timeframes. Since the launch of Puppet Core in February 2025, a total of 67 unique Common Vulnerabilities and Exposures (CVEs) have been evaluated and addressed — including 4 rated as Critical severity and 20 rated as High severity.

CVSS v3.1 Scoring Overview

CVEs are evaluated using the Common Vulnerability Scoring System (CVSS), with severity levels assigned through the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST). The table below shows how CVSS numeric ranges map to severity categories (Low, Medium, High, Critical) and provides a general description of the potential impact at each level.

Score Range	Severity Level	General Impact Description
0.0	None	No impact on confidentiality, integrity, or availability.
0.1 – 3.9	Low	Minimal impact. Exploitation is unlikely to significantly compromise a system.
4.0 – 6.9	Medium	Moderate impact. Vulnerabilities may lead to limited compromise or DoS.
7.0 – 8.9	High	Severe impact. Exploitation can result in major disruption or significant data loss.
9.0 – 10.0	Critical	Complete compromise of systems and data is likely with minimal effort.

Summary of Remediated Puppet Core CVEs by Version & Severity

This table highlights the number of CVEs remediated in each Puppet Core release. With vendor-backed remediation and guaranteed SLAs, Puppet Core helps enterprises reduce security risk and maintain continuous compliance — benefits not available with unsupported open source solutions.

Version	Critical	High	Medium	Low	Not Specified	Not Applicable
8.18.0	0	2	5	2	0	0
8.17.0	1	3	10	2	0	0
8.16.0	0	2	4	1	0	0
8.15.0	0	3	0	0	0	0
8.14.0	2	2	1	1	3	0
8.13.0	1	6	2	2	2	0
8.12.0	0	2	0	1	3	0
8.11.0	0	0	1	0	0	3
Total	4	20	23	9	8	3

The following pages outline the CVEs addressed in each Puppet Core release, referencing the CVSS scoring system to indicate severity and impact.

If you have technical questions about any release of Puppet Core, please open a support ticket:

[SUPPORT PORTAL](#)

For information on all Perforce Puppet products, contact your Account Manager or visit:

[VISIT WEBSITE](#)

CVEs Remediated in Puppet Core 8.18.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Impact Summary	Potential Impact
zlib	CVE-2026-27820	8.8	High	Memory Corruption	Successful exploitation could cause application failures or unexpected behavior, increasing downtime risk and potentially impacting the integrity of managed systems.
curl	CVE-2026-3805	7.5	High	Service Crash	Triggering this issue could cause automation tasks or supporting services to fail unexpectedly, resulting in outages and reduced operational reliability.
curl	CVE-2026-1965	6.5	Medium	Unauthorized Access	Incorrect credential handling could allow actions to be performed under the wrong identity, increasing the risk of policy violations, audit findings, or unauthorized changes.
curl	CVE-2026-3784	6.5	Medium	Authentication Bypass	Improper credential reuse may enable unintended access through shared infrastructure components, weakening security controls and trust boundaries.
libxml2	CVE-2026-1757	6.2	Medium	Denial of Service	Abuse of this flaw could exhaust system resources, resulting in service crashes that interrupt automation runs and increase recovery and remediation effort.

CVEs Remediated in Puppet Core 8.18.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Impact Summary	Potential Impact
libxml2	CVE-2026-0990	5.9	Medium	Service Disruption	An attacker could repeatedly disrupt services that rely on XML processing, leading to outages that affect configuration enforcement and routine infrastructure operations.
curl	CVE-2026-3783	5.3	Medium	Credential Exposure	Exposure of authentication tokens could allow unauthorized access to downstream services, increasing security risk and potential compliance concerns.
libxml2	CVE-2026-0989	3.7	Low	Denial of Service	Exploiting this issue could cause automation services to become unstable or unavailable, increasing the risk of interruptions in system management and operational workflows.
libxml2	CVE-2026-0992	2.9	Low	Resource Exhaustion	Left unaddressed, this vulnerability could degrade system performance over time, reducing the reliability of automation processes that depend on consistent execution.

CVEs Remediated in Puppet Core 8.17.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Impact Summary	Potential Impact
OpenSSL 3.0	CVE-2025-15467	9.8	Critical	System Takeover	A remote attacker could crash the service by sending a specially crafted message. In some cases, this could also allow the attacker to run their own code on the system.
OpenSSL 3.0	CVE-2025-69420	7.5	High	Service Disruption	An attacker could send malformed timestamp responses that cause verification services to repeatedly crash, leading to service outages.
OpenSSL 3.0	CVE-2025-69421	7.5	High	Certificate Outage	Processing a malicious certificate bundle could crash systems that handle certificates, interrupting certificate management and automation workflows.
OpenSSL 3.0	CVE-2025-69419	7.4	High	Memory Corruption	A crafted certificate file could corrupt application memory, typically causing the service to crash and become unavailable.
curl 8.17.0	CVE-2025-14017	6.3	Medium	Encryption Weakness	In certain multi-threaded setups, encrypted directory traffic could be exposed to interception or tampering due to weakened TLS settings.

CVEs Remediated in Puppet Core 8.17.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Impact Summary	Potential Impact
curl 8.17.0	CVE-2025-13034	5.9	Medium	Malicious Connection	Under specific conditions, the system may connect to an impostor server without detecting it, increasing the risk of data interception.
OpenSSL 3.0	CVE-2026-22795	5.5	Medium	Certificate Disruption	A malformed certificate file could trigger a crash in services that process certificate bundles, resulting in avoidable downtime.
OpenSSL 3.0	CVE-2026-22796	5.3	Medium	Signature Disruption	Malicious signed data could cause signature verification processes to crash, disrupting validation and trust checks.
Ruby 3.2	CVE-2025-58767	5.3	Medium	Signature Disruption	Malicious signed data could cause signature verification processes to crash, disrupting validation and trust checks.
curl 8.17.0	CVE-2025-14524	5.3	Medium	Resource Consumption	Specially crafted XML input could consume excessive system resources, slowing down or crashing the affected service.
curl 8.17.0	CVE-2025-14819	5.3	Medium	Credential Exposure	Authentication tokens could be unintentionally sent to another system during redirects, allowing attackers to reuse exposed credentials.

CVEs Remediated in Puppet Core 8.17.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Impact Summary	Potential Impact
curl 8.17.0	CVE-2025-15079	5.3	Medium	SSH Host Spoofing	SSH connections may succeed to hosts that are not explicitly approved, increasing the risk of connecting to spoofed systems.
OpenSSL 3.0	CVE-2025-68160	4.7	Medium	Memory Corruption	Under specific conditions, memory corruption could occur and cause the application to crash, leading to a loss of service.
OpenSSL 3.0	CVE-2025-69418	4.0	Medium	Data Exposure	Small portions of encrypted data may not be protected, allowing attackers to read or alter those bytes without detection.
curl 8.17.0	CVE-2025-15224	3.1	Low	SSH Authentication Exposure	SSH transfers could authenticate using unintended credentials, potentially allowing actions to occur under the wrong identity.
Ruby 3.2	CVE-2025-61594	2.7 (v4.0)	Low	Credential Exposure	Credentials embedded in URLs could be unintentionally carried over and exposed to logs or external systems.

CVEs Remediated in Puppet Core 8.16.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
OpenSSL	CVE-2025-9230	7.5	High	Out-of-bounds read/write in CMS password-recipient info handling. Could lead to memory corruption or code execution, albeit low probability.
Curl (libcurl)	CVE-2025-9086	7.5	High	Out-of-bounds read when transitioning from HTTPS to HTTP for a secure cookie path, potentially allowing override of secure cookies.
OpenSSL (HTTP client no_proxy IPv6)	CVE-2025-9232	5.9	Medium	Out-of-bounds read in HTTP client API when no_proxy env var is set and authority uses IPv6 — crash/DoS possible.
REXML (Ruby gem)	CVE-2025-58767	5.3	Medium	Denial-of-Service vulnerability when parsing XML containing multiple XML declarations.
Curl (WebSocket mask)	CVE-2025-10148	5.3	Medium	WebSocket mask predictable (fixed mask) instead of varying per frame; may allow malicious server to poison proxy cache.
URI gem (Ruby)	CVE-2025-61594	5.1	Medium	When using the + operator to combine URIs, sensitive information (such as credentials) from the original URI may be leaked.
Thor gem (Ruby)	CVE-2025-54314	2.8	Low	Version before 1.4.0 of the Thor gem can construct an unsafe shell command from library input (though the supplier disputes exploitability).

CVEs Remediated in Puppet Core 8.15.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
libxslt	CVE-2025-7424	7.5	High	Type confusion leads to crashes, corrupt memory or denial of service.
libxslt	CVE-2025-7425	7.8	High	A flaw in the process of attribute type, atype, flags can result in corruption of memory which can causes crashes, use after free access or heap corruption.
resolv gem	CVE-2025-24294	7.5	High	Potential denial of service due to an insufficient length check with an DNS packet.

CVEs Remediated in Puppet Core 8.14.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
libxml2	CVE-2025-49794	9.1	Critical	heap use after free (uaf) leads to denial of service (dos)
libxml2	CVE-2025-49796	9.1	Critical	type confusion leads to denial of service (dos)
libxml2	CVE-2025-6021	7.5	High	integer overflow in xmlbuildqname() leads to stack buffer overflow in libxml2
libxml2	CVE-2025-49795	7.5	High	null pointer dereference leads to denial of service (dos)
net-imap	CVE-2025-43857	6	Medium	rubygem vulnerable to possible DoS by memory exhaustion
libxml2	CVE-2025-6170	2.5	Low	stack buffer overflow in xmllint interactive shell command handling
curl	CVE-2025-5025	Not specified	Not specified	No QUIC certificate pinning with wolfSSL
curl	CVE-2025-4947	Not specified	Not specified	QUIC certificate check skip with wolfSSL
curl	CVE-2025-5399	Not specified	Not specified	WebSocket endless loop

CVEs Remediated in Puppet Core 8.13.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
curl	CVE-2025-0665	9.8	Critical	Double close of eventfd leads to DoS.
Ruby	CVE-2025-27220	7.5	High	Regex DoS in `Util#escapeElement` method of CGI.
curl	CVE-2025-0725	7.3	High	Integer overflow in gzip decompression.
libxml2	CVE-2025-24928	7.8	High	Use-after-free in ID constraints processing.
libxml2	CVE-2024-56171	7.8	High	Use-after-free in schema validation.
libxslt	CVE-2024-55549	7.8	High	Use-after-free in `xsltGetInheritedNsList`.
libxslt	CVE-2025-24855	7.8	High	Use-after-free during nested XPath evaluation.
Ruby	CVE-2025-27219	5.8	Medium	DoS in `CGI::Cookie.parse` due to no length limit.
OpenSSL	CVE-2025-0306	6.5	Medium	Marvin Attack risk via crafted TLS exchanges.
Ruby	CVE-2025-27221	3.2	Low	Credential leakage due to userinfo persistence.
OpenSSL	CVE-2024-13176	4.7	Low	Timing side-channel in ECDSA nonce.
Puppet Core	CVE-2024-9128	Not specified	Not specified	Prevents unintended trust relationships when running unprivileged.
curl	CVE-2025-0167	Not specified	Not specified	Credential leakage with `.netrc` and redirects.

CVEs Remediated in Puppet Core 8.12.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
libxml2	CVE-2025-32415	7.5	High	Heap-based buffer under-read in xmlschemas.c.
rapidjson	CVE-2024-38517	7.8	High	Integer overflow leading to EoP.
augeas	CVE-2025-2588	3.3	Low	Null pointer dereference in re_case_expand.
libxml2	CVE-2025-32411	Not specified	Not specified	libxml2 updated to 2.13.8 to address vulnerability.
boost	CVE-2012-2677	Not specified	Not specified	boost updated to address CVE.
rapidjson	CVE-2024-39684	Not specified	Not specified	Integer overflow in ParseNumber().

CVEs Remediated in Puppet Core 8.11.0

View information on this version of Puppet Core:

WHAT'S NEW

Affected Library	CVE ID	CVSS v3.1 Score	Severity	Description
REXML	CVE-2024-49761	5.3	Medium	REXML DoS via crafted XML documents.
Evaluated CVEs	CVE-2025-0167	Not applicable	Not applicable	Determined to be not impactful to Puppet Core.
Evaluated CVEs	CVE-2025-0665	Not applicable	Not applicable	Determined to be not impactful to Puppet Core.
Evaluated CVEs	CVE-2025-0725	Not applicable	Not applicable	Determined to be not impactful to Puppet Core.