



CVE-2023-2530

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

Summary

CVE	CVE-2023-2530
State	PUBLIC
Assigner	security@puppet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 20:15:00 UTC
Updated	2023-11-07 04:12:00 UTC
Description	A privilege escalation allowing remote code execution was discovered in the orchestration service.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Puppet	Puppet Enterprise	2023.0	All	All	All
Application	Puppet	Puppet Enterprise	2023.1.0	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-2530 Remote Code Execution in Orchestrator Puppet by Perforce	MISC	www.puppet.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378697 Puppet Enterprise Remote Code Execution (RCE) Vulnerability

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