



CVE-2023-33191

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

Summary

CVE	CVE-2023-33191
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-30 07:15:00 UTC
Updated	2023-06-05 16:44:00 UTC
Description	Kyverno is a policy engine designed for Kubernetes. Kyverno seccomp control can be circumvented. Users of the podSecu

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nirmata	Kyverno	All	All	All	All

References

Reference	Source	Link
Seccomp control can be circumvented when using validate.podSecurity subrule · Advisory · kyverno/kyverno · GitHub	MISC	github.com
Release v1.9.4 · kyverno/kyverno · GitHub	MISC	github.com
fix: PSa latest version check by realshuting · Pull Request #7263 · kyverno/kyverno · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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

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