Kyverno: ServiceAccount token leaked to external servers via apiCall service URL

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41323
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 04:16:20 UTC
Updated	2026-04-24 14:50:56 UTC
Description	Kyverno is a policy engine designed for cloud native platform engineering teams. Prior to versions 1.18.0-rc1, 1.17.2-rc1, ar

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from security-advisories@github.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Problem Types: CWE-200 | CWE-918 | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kyverno	Kyverno	affected < 1.16.4	Not specified
CNA	Kyverno	Kyverno	affected >= 1.17.0-rc1, < 1.17.2-rc1	Not specified

References

Reference	Source	Link
github.com/kyverno/kyverno/commit/f70e8ac1e7acd2e3844f9553e4a884f07f953de0	security-advisories@github.com	github.co
github.com/kyverno/kyverno/security/advisories/GHSA-f9g8-6ppc-pqq4	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.co
github.com/kyverno/kyverno/commit/bc4f91c4801b1eaa2edc0a14e2f1b0af8cf0c1f5	security-advisories@github.com	github.co
github.com/kyverno/kyverno/commit/c2eab00033e635bda4e4efb58c1b472b41728bb6	security-advisories@github.com	github.co
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.