



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

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

## Summary

<b>CVE</b>	CVE-2026-41323
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 04:16:20 UTC
<b>Updated</b>	2026-04-24 14:50:56 UTC
<b>Description</b>	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

Integrity

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.com
github.com/kyverno/kyverno/security/advisories/GHSA-f9g8-6ppc-pqq4	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/kyverno/kyverno/commit/bc4f91c4801b1eaa2edc0a14e2f1b0af8cf0c1f5	security-advisories@github.com	github.com
github.com/kyverno/kyverno/commit/c2eab00033e635bda4e4efb58c1b472b41728bb6	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)