



CVE-2022-36089

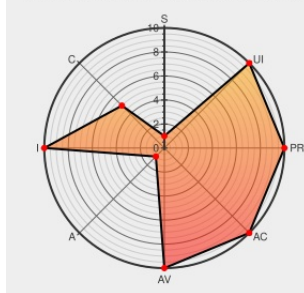
Published on: Not Yet Published

Last Modified on: 09/16/2022 04:19:00 PM UTC

CVE-2022-36089 - advisory for GHSA-cq42-w295-r29q

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N



Certain versions of [Kubevela](#) from [Kubevela](#) contain the following vulnerability:

KubeVela is an application delivery platform Users using KubeVela's VelaUX APIServer could be affected by an authentication bypass vulnerability. In KubeVela prior to versions 1.4.11 and 1.5.4, VelaUX APIServer uses the `PlatformID` as the signed key to generate the JWT tokens for users. Another API called `getSystemInfo` exposes the platformID. This vulnerability allows users to use the platformID to re-generate the JWT tokens to bypass the authentication. Versions 1.4.11 and 1.5.4 contain a patch for this issue.

CVE-2022-36089 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Kubevela](#) - **kubevela** version $\geq 1.4.0$, $< 1.4.11$

Affected Vendor/Software: [Kubevela](#) - **kubevela** version $\geq 1.5.0$, $< 1.5.3$

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Fix: fix signedKey using platform id by FogDong · Pull Request #4634 · kubevela/kubevela · GitHub	github.com text/html	MISC github.com/kubevela/kubevela/pull/4634
Authentication Bypass by Capture-replay in VelaUX APIServer · Advisory · kubevela/kubevela · GitHub	github.com text/html	CONFIRM github.com/kubevela/kubevela/security/advisories/GHSA-cq42-w295-r29q

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubevela	Kubevela	All	All	All	All
cpe:2.3:a:kubevela:kubevela:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36089 : KubeVela is an application delivery platform Users using KubeVela's VelaUX APIServer could be affe... twitter.com/i/web/status/1...	2022-09-07 23:05:35
 /r/netcve	CVE-2022-36089	2022-09-07 23:38:18

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)