CYBER ADVISORY

TLP:CLEAR

27 March 2025

Kubernetes Vulnerabilities Impacting Ingress-NGINX Controller

Kubernetes | RCE | Ingress-NGINX | Proof of Concept

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical, high, and medium vulnerabilities in Ingress NGINX controller for Kubernetes. The vulnerabilities disclosed can be chained together to facilitate a cluster takeover with no credential or administrative access required.[1] Additionally, a proof of concept has been published for the most critical of the vulnerabilities disclosed (CVE-2025-1974).[2][3]

Title	CVE (CVSS Score)	Description	Affected Versions
Ingress-Nginx Admission Controller RCE Escalation[4]	CVE-2025-1974 (**9.8**)	A security issue was discovered in Kubernetes where under certain conditions, an unauthenticated user with access to the pod network can achieve arbitrary code execution in the context of the ingress-nginx controller. This can lead to disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	<v1.11.0 v1.11.0 - 1.11.4 v1.12.0
Ingress-Nginx Controller - Configuration Injection Via Unsanitized Auth-Url Annotation[5]	CVE-2025-24514 (**8.8**)	A security issue was discovered in ingress-nginx where the auth-url Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	< 1.11.5 >= 1.12.0-beta.0, < 1.12.1

Ingress-Nginx Controller - Configuration Injection Via Unsanitized Mirror Annotations[6]	CVE-2025-1098 (**8.8**)	A security issue was discovered in ingress-nginx where the mirror-target and mirror-host Ingress annotations can be used to inject arbitrary configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	< 1.11.5 >= 1.12.0-beta.0, < 1.12.1
Ngress-Nginx Controller - Configuration Injection Via Unsanitized Auth-Tls-Match-Cn Annotation[7]	CVE-2025-1097 (**8.8**)	A security issue was discovered in ingress-nginx where the auth-tls-match-cn Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	< 1.11.5 >= 1.12.0-beta.0, < 1.12.1
Ingress-Nginx Controller - Auth Secret File Path Traversal Vulnerability[8]	CVE-2025-24513 (**4.8**)	A security issue was discovered in ingress-nginx where attacker-provided data are included in a filename by the ingress-nginx Admission Controller feature, resulting in directory traversal within the container. This could result in denial of service, or when combined with other vulnerabilities, limited disclosure of Secret objects from the cluster.	< 1.11.5 >= 1.12.0-beta.0, < 1.12.1

Recommendation:

The Cal-CSIC recommends immediately upgrading Ingress-nginx to the latest version.

For more information on applying the security updates please refer to the Kubernetes Security Advisory.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled using the direct vendor information and from a variety of trusted security research blogs and cybersecurity news websites.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Kubernetes; "Ingress-nginx CVE-2025-1974: What You Need to Know"; https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1974/; accessed 26 March 2025.
[2] Wiz; "IngressNightmare: 9.8 Critical Unauthenticated Remote Code Execution Vulnerabilities in Ingress NGINX"; https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities; accessed 26 March 2025.
[3] Github; "CVE-2025-1974/exploit.py"; https://github.com/yoshino-s/CVE-2025-1974/blob/main/exploit.py; accessed 26 March 26, 2025.
[4] Github; "CVE-2025-1974: ingress-nginx admission controller RCE escalation #131009"; https://github.com/kubernetes/kubernetes/issues/131009; accessed 26 March 26, 2025.
[5] Github; "ingress-nginx controller - configuration injection via unsanitized auth-url annotation"; https://github.com/advisories/GHSA-fwwp-xcxw-39vq; accessed 26 March 26, 2025.
[6] Github; "ingress-nginx controller - configuration injection via unsanitized mirror annotations"; https://github.com/advisories/GHSA-vg63-w3p9-jc9m; accessed 26 March 26, 2025.
[7] Github; "ngress-nginx controller - configuration injection via unsanitized auth-tls-match-cn annotation"; https://github.com/advisories/GHSA-823x-fv5p-h7hw; accessed 26 March 26, 2025.
[8] Github; "ingress-nginx controller - auth secret file path traversal vulnerability"; https://github.com/advisories/GHSA-242m-6h72-7hgp; accessed 26 March 26, 2025.