ARBITRARY CODE EXECUTION VULNERABILITY IN INGRESS-NGINX CONTROLLER

Vairav CVE Report

Date: March 25, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Wiz Research has identified a critical security threat, “IngressNightmare,” affecting the Ingress NGINX Controller for Kubernetes. Assigned CVEs **CVE-2025-1097, CVE-2025-1098, CVE-2025-24514,** and **CVE-2025-1974**, these vulnerabilities enable unauthenticated remote code execution (RCE), potentially leading to complete cluster takeover. Organizations using affected versions must take immediate action to mitigate the risk.

VULNERABILITY DETAILS

CVE-2025-24514: Ingress-Nginx Controller - Configuration Injection Via Unsanitized Auth-Url Annotation

Description: A security issue in ingress-nginx allows the auth-url Ingress annotation to inject configuration, enabling arbitrary code execution in the controller and exposing Secrets.

Impact: Arbitrary code execution.

CVSS Score: 8.8

CVE-2025-1097: Ingress-Nginx Controller - Configuration Injection Via Unsanitized Auth-Tls-Match-Cn Annotation

Description: A vulnerability in ingress-nginx allows attackers to exploit the auth-tls-match-cn annotation to inject unauthorized configurations into NGINX, potentially leading to arbitrary code execution and unauthorized access to Secrets.

Impact: Arbitrary code execution.

CVSS Score: 8.8

CVE-2025-1098: Ingress-Nginx Controller - Configuration Injection Via Unsanitized Mirror Annotations

Description: A security flaw in ingress-nginx allows the mirror-target and mirror-host annotations to inject arbitrary configuration, enabling code execution in the controller and exposure of Secrets

Impact: Arbitrary code execution.

CVSS Score: 8.8

CVE-2025-1974: Ingress-Nginx Admission Controller RCE Escalation

Description: A security issue in Kubernetes allows an unauthenticated attacker with pod network access to execute arbitrary code in the ingress-nginx controller, leading to potential exploitation.

Impact: Arbitrary code execution.

CVSS Score: 9.8

AFFECTED VERSIONS

Ingress NGINX Controller versions:

- 0 through 1.11.4
- 1.12.0

EXPLOIT DETAILS

These vulnerabilities allow attackers to inject arbitrary NGINX directives into ingress configurations. Exploiting the ssl_engine directive, attackers can execute arbitrary shared libraries, enabling full control over Kubernetes clusters. Attackers can also exploit misconfigured validating admission webhooks, leading to unauthorized configuration modifications and secret exfiltration.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Upgrade to Ingress NGINX Controller v1.12.1 or v1.11.5 immediately.

ADDITIONAL SECURITY MEASURES

- Restrict access to the validating admission webhook via network policies.
- Disable the admission controller if an immediate upgrade is not feasible.
- Implement firewall rules to limit unauthorized access to Kubernetes control plane services.
- Identify active Ingress NGINX pods: kubectl get pods --all-namespaces --selector app.kubernetes.io/name=ingress-nginx

REFERENCES

https://securityonline.info/cve-2025-1974-cvss-9-8-ingress-nginx-flaws-threaten-mass-kubernetes-compromise/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com