Security Advisory 2025-012

Critical Vulnerabilities in Kubernetes Ingress-NGINX

2025-03-25 — v1.0

TLP:CLEAR

History:

- *25/03/2025 — v1.0 – Initial publication*

Summary

On March 24, 2025, Wiz Research disclosed a set of critical Remote Code Execution vulnerabilities in the Ingress-NGINX Controller for Kubernetes. The vulnerabilities **CVE-2025-1097**, **CVE-2025-1098**, **CVE-2025-24514**, and **CVE-2025-1974** can be exploited to gain full cluster access, resulting in a complete compromise of the environment [1,2].

The vulnerabilities affect a widely used component in Kubernetes environments responsible for routing external traffic to internal services. Clusters with publicly exposed admission webhooks are at immediate risk.

Technical Details

The vulnerability **CVE-2025-1097**, with a CVSS score of 8.8, allows an unauthenticated remote attacker to inject configuration into nginx using the `auth-tls-match-cn` Ingress annotation. 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.)

The vulnerability **CVE-2025-1098**, with a CVSS score of 8.8, allows an unauthenticated remote attacker arbitrary configuration into nginx using the `mirror-target` and `mirror-host` Ingress annotations. 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.)

The vulnerability **CVE-2025-24514**, with a CVSS score of 8.8, allows an unauthenticated remote attacker to inject configuration into nginx using the `auth-url` Ingress annotation. 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.)

The vulnerability **CVE-2025-1974**, with a CVSS score of 9.8, is security issue in Kubernetes where under certain conditions, an unauthenticated attacker 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.)

Successful exploitation of these vulnerabilities may allow attackers to:

- Execute arbitrary code
- Access all cluster secrets across namespaces
- Take full control over the Kubernetes cluster

Affected Products

The following versions of the Ingress-NGINX Controller are affected:

- all versions prior to v1.11.0;
- versions prior to 1.12.1;
- versions prior to 1.11.5.

Recommendations

CERT-EU recommends updating to Ingress-NGINX Controller as soon as possible and ensuring the admission webhook endpoint is not exposed on the Internet, or any other untrusted source.

Workarounds

If upgrading immediately is not possible, the following actions are strongly advised:

- Restrict network access to the admission controller to allow only connections from the Kubernetes API server.
- Temporarily disable the admission controller component of Ingress-NGINX

References

[1] https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities

[2] https://groups.google.com/g/kubernetes-security-announce/c/2qa9DFtN0cQ