مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical RCE Vulnerabilities in Ingress NGINX Controller for Kubernetes

Tracking #:432317008

Date:25-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new set of critical security vulnerabilities, collectively dubbed “IngressNightmare”, has been discovered in the Ingress NGINX Controller for Kubernetes.

TECHNICAL DETAILS:

A critical vulnerability chain dubbed IngressNightmare (CVSS 9.8) has been discovered in the Kubernetes Ingress-NGINX Controller, enabling unauthenticated attackers to execute remote code (RCE) and compromise entire clusters.

These flaws, tracked as CVE-2025-1097, CVE-2025-1098, CVE-2025-24514, and CVE-2025-1974, enable unauthenticated remote code execution (RCE) attacks, potentially leading to full Kubernetes cluster compromise. With a CVSS score of 9.8, these vulnerabilities allow attackers to exploit insecure Ingress NGINX configurations, gaining unauthorized access to all secrets stored across namespaces, effectively leading to cluster-wide takeover.

Vulnerability Breakdown

1. **CVE-2025-24514 (CVSS 8.8)** – Enables **configuration injection** via a malicious **auth-url annotation**.
2. **CVE-2025-1097 (CVSS 8.8)** – Leverages the **auth-tls-match-cn** directive to manipulate **regex-based configurations**.
3. **CVE-2025-1098 (CVSS 8.8)** – Exploits the **Ingress object UID** to inject malicious payloads.
4. **CVE-2025-1974 (CVSS 9.8)** – The most severe of the four, utilizes an undocumented **ssl_engine directive** in OpenSSL to load and execute **arbitrary shared libraries**.

Exploit Chain

1. **Configuration Injection**: Attackers send malicious AdmissionReview requests to the admission controller, exploiting unsanitized input fields (e.g., auth-url)
2. **File Descriptor Hijacking**: Oversized HTTP requests upload payloads to NGINX’s client body buffers. Even after deletion, file descriptors remain accessible via /proc/[PID]/fd/[FD]
3. **Shared Library Execution**: The ssl_engine directive loads the attacker’s library, executing code with the pod’s high-privileged service account
4. **Cluster Takeover**: Compromised pods grant access to **all Kubernetes secrets**, enabling lateral movement and full control.

RECOMMENDATIONS:

- Patch to Ingress NGINX Controller v1.12.1 or v1.11.5.
- Restrict Network Access:Implement network policies to block access to the admission webhook.
- Disable the Admission Controller (Temporary Fix):If an upgrade isn’t possible, consider disabling the admission controller until patches can be applied.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/kubernetes/ingress-nginx