Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

IngressNightmare Isn't Just a Bug, It's a Blueprint for Breach

Date of Publication

April 9, 2025

Admiralty Code

A1

TA Number

TA2025107

Summary

First Reported: December 31, 2024
Affected Product: Ingress NGINX Controller for Kubernetes
Impact: Over 6,500 Kubernetes clusters are at risk after the discovery of IngressNightmare a set of four critical flaws in the Ingress NGINX Controller that allow unauthenticated attackers to remotely execute code and hijack entire environments. One crafted request is all it takes to slip past defenses, seize secrets, and take over the cluster. It's a wake-up call for cloud security when one overlooked component cracks, the whole system can crumble.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	MICRO PATCH
CVE-2025-1974	IngressNightmare (Kubernetes Unauthenticated Remote Code Execution Vulnerability)	Ingress NGINX Controller for Kubernetes	✗	✗	✓
CVE-2025-1097	IngressNightmare (Kubernetes Arbitrary Code Execution Vulnerability)	Ingress NGINX Controller for Kubernetes	✗	✗	✓
CVE-2025-1098	IngressNightmare (Kubernetes Code Execution Vulnerability)	Ingress NGINX Controller for Kubernetes	✗	✗	✓
CVE-2025-24514	IngressNightmare (Kubernetes Command Injection Vulnerability)	Ingress NGINX Controller for Kubernetes	✗	✗	✓
CVE-2025-24513	Kubernetes Directory Traversal Vulnerability	Ingress NGINX Controller for Kubernetes	✗	✗	✓

Vulnerability Details

#1

A set of four high-impact vulnerabilities has been uncovered in the Ingress NGINX Controller for Kubernetes, exposing over 6,500 clusters to unauthenticated remote code execution. Publicly accessible and widely deployed, the affected component puts more than 40% of cloud environments at immediate risk of complete cluster takeover.

#2

These flaws CVE-2025-1097, CVE-2025-1098, CVE-2025-24514, and the critical CVE-2025-1974 are collectively known as ***IngressNightmare***. Exploiting them allows attackers to execute arbitrary code and access all Kubernetes secrets across all namespaces, without authentication. The weakness lies in the admission controller, a component inside the Ingress NGINX pod that validates ingress objects.

#3

By default, it's network-exposed and lacks authentication and open door. When it receives an ingress object, it builds a NGINX config and validates it using the NGINX binary. But a flaw in this phase lets attackers inject a crafted config, triggering remote code execution during validation.

#4

With elevated privileges and unrestricted access, the admission controller becomes an ideal escalation point. Once compromised, the attacker can sweep through the cluster, harvesting secrets and gaining complete control. Specifically, CVE-2025-24513 and CVE-2025-24514 can leak sensitive secrets, while CVE-2025-1097 and CVE-2025-1098 further expand the attack surface.

#5

CVE-2025-1974 is the most severe, enabling cluster-wide compromise via configuration injection. IngressNightmare is a stark reminder that when core components like ingress controllers go unpatched or misconfigured, the blast radius can be massive.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-1974	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*:*:*	CWE-653
CVE-2025-1097			CWE-20
CVE-2025-1098			CWE-20
CVE-2025-24514			CWE-20
CVE-2025-24513			CWE-20

Recommendations

Immediately Detection & Upgrade to a Patched Version: Begin by verifying whether your clusters are utilizing ingress-nginx. In most scenarios, this can be confirmed by executing the following command with at least cluster-scoped read-only permissions:
kubectl get pods --all-namespaces --selector app.kubernetes.io/name=ingress-nginx

Update to Ingress NGINX Controller v1.12.1, v1.11.5, or later to eliminate the vulnerabilities at their source.

Temporary Mitigation Measures for Unpatched Clusters: If upgrading isn't immediately possible, apply the following steps to reduce risk:

- Restrict access to the admission controller by enforcing network policies that allow only the Kubernetes API Server to communicate with it.
- Temporarily disable the admission controller:
  - For Helm users, reinstall with *controller.admissionWebhooks.enabled=false*
  - For manual setups, delete the *ValidatingWebhookConfiguration* named ingress-nginx-admission and remove the --validating-webhook argument from the controller's Deployment or DaemonSet.
- Once the controller is upgraded, re-enable the admission controller to restore essential ingress validation.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0040** Impact	**T1190** Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	**T1203** Exploitation for Client Execution	**T1546** Event Triggered Execution	**T1068** Exploitation for Privilege Escalation
T1211 Exploitation for Defense Evasion	**T1526** Cloud Service Discovery	**T1552.001** Credentials In Files	**T1496** Resource Hijacking

Patch Details

Organizations should upgrade the Ingress NGINX Controller to version v1.12.1, v1.11.5, or a later release to effectively eliminate the underlying vulnerabilities and prevent exploitation.

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

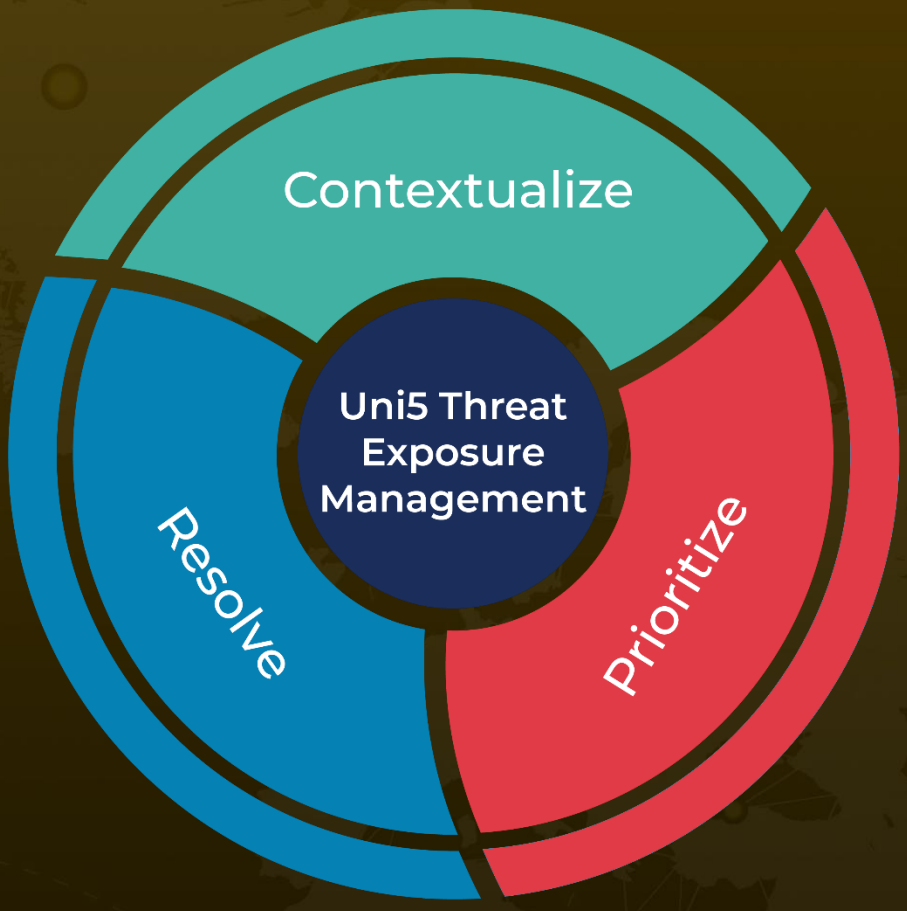
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 9, 2025 • 9:30 PM

More at www.hivepro.com