ADV2025_111 Kubernetes Security Advisory (3rd April 2025)

Kubernetes has published a security advisory to address vulnerabilities affecting the following products on March 24, 2025. It is recommended that you take the necessary precautions to ensure your products are always protected.

- Kubernetes ingress-nginx controller — versions prior to 1.11.5
- Kubernetes ingress-nginx controller — versions prior to 1.12.1

For more information on these updates, you can follow these URLs:

1. https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1974/
2. https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.11.5
3. https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.12.1
4. https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.11.5
5. https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities
6. https://aws.amazon.com/security/security-bulletins/AWS-2025-006/
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24514
8. https://cloud.google.com/support/bulletins
9. https://thehackernews.com/2025/03/critical-ingress-nginx-controller.html

This vulnerability allows unauthenticated RCE and wide access to secrets. The vulnerability is rated a CVSS 9.8 and is tracked with the following identifiers: CVE-2025-1097, CVE-2025-1098, CVE-2025-24514 and CVE-2025-1974.

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Kubernetes Blog. (2025, March 24). Retrieved from Kubernetes. https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1974/
- Kubernetes security advisory. (2025, March 27). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/kubernetes-security-advisory-av25-161-update-1