An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2503250145

NCSC Advisory

Critical Vulnerabilities found in Kubernetes Ingress-NGINX
CVE-2025-1974

25th, March 2025

STATUS: TLP:CLEAR

Description

CVE ID: CVE-2025-1974

Published: 2025-03-24

Vendor: Kubernetes

Product: Ingress-NGINX

CVSS Score[1]: 9.8

Products Affected

Product	Version
Ingress-NGINX	0 <= 1.11.4
Ingress-NGINX	1.12.0

Impact

A security issue tracked as **CVE-2025-1974**, has been discovered 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.)

Four additional CVEs were also discovered in the same affected versions of ingress-nginx:

- **CVE-2025-1097 (CVSS 8.8)**: The `auth-tls-match-cn` Ingress annotation can be used to inject configuration into nginx.
- **CVE-2025-1098 (CVSS 8.8)**: The `mirror-target` and `mirror-host` Ingress annotations can be used to inject arbitrary configuration into nginx.
- **CVE-2025-24514 (CVSS 8.8)**: The `auth-url` Ingress annotation can be used to inject configuration into nginx.

These three vulnerabilities could lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller.

[1] https://www.first.org/cvss/

- **CVE-2025-24513 (CVSS 4.8)**: Attacker-provided data included in a filename by the ingress-nginx Admission Controller feature could result in directory traversal within the container.

Common Weakness Enumeration (CWE)[2]:

- CWE-653: Improper Isolation or Compartmentalization (CVE-2025-1974)
- CWE-20: Improper Input Validation (CVE-2025-1097, CVE-2025-1098, CVE-2025-24514, CVE-2025-24513)

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

Kubernetes have patched all vulnerabilities in Ingress NGINX Controller versions 1.12.1 and 1.11.5.

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Kubernetes.

- https://nvd.nist.gov/vuln/detail/CVE-2025-1974
- https://www.cve.org/CVERecord?id=CVE-2025-1974
- https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1974/
- https://github.com/kubernetes/kubernetes/issues/131009

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog