مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NeuVector

Tracking #:432317669

Date:03-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in NeuVector, an open-source container security platform for Kubernetes environments. This flaw could potentially expose administrative access to unauthorized users within the cluster environment

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2025-8077
- CVSS Score 9.8 Critical
- A critical vulnerability exists in NeuVector versions 5.0.0 through 5.4.5. The flaw arises due to the use of a fixed default password for the built-in admin account when the bootstrap password is not properly retrieved from a Kubernetes Secret. Exploitation of this vulnerability could allow attackers to obtain administrative access to NeuVector within a containerized environment.
- Vulnerability Type: Hardcoded/fixed default password
- Root Cause: NeuVector falls back to a static default password if the neuvector-bootstrap-secret is not available during initialization.
- Impact: Any workload or user with network access to NeuVector's API within the cluster can authenticate using the default credentials. Once logged in, attackers may generate authentication tokens and invoke privileged API operations.
- Exploitability:
    - Network accessible within the cluster
    - No authentication or privileges required
    - Low complexity (simple valid login with known credentials)

Affected Versions

- NeuVector 5.0.0 – 5.4.5

Fixed Versions

- NeuVector 5.4.6 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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/neuvector/neuvector/security/advisories/GHSA-8pxw-9c75-6w56