مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Kubernetes Image Builder

Tracking #:432317516

Date:22-07-2025

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 high-severity vulnerability in Kubernetes Image Builder project that could allow attackers to gain unauthorized root-level access on Windows nodes.

TECHNICAL DETAILS:

A high-severity vulnerability has been disclosed in the Kubernetes Image Builder project that could allow attackers to gain unauthorized root-level access on Windows nodes. Tracked as **CVE-2025-7342**, this flaw impacts virtual machine images built using the **Nutanix** or **OVA** providers in Image Builder versions **v0.1.44 and earlier**.

Vulnerability Details:

- **CVE-2025-7342**
- CVSS Score 8.1 High
- The affected versions of Kubernetes Image Builder include default Windows Administrator credentials in generated virtual machine images when the user does not explicitly override them during the build process.
- Clusters deploying Windows nodes from unpatched images are vulnerable to unauthorized remote access. An attacker with network access can log in using default credentials, escalate privileges, and potentially compromise the entire cluster.

Affected Versions:

- v0.1.44 and earlier

Fixed Versions:

- v0.1.45 or later

RECOMMENDATIONS:

- **Audit Existing Images:**
  Review all Windows VM images built using Kubernetes Image Builder with Nutanix or OVA providers. If default credentials are present, treat these systems as compromised until validated.
- **Upgrade Image Builder:**
  Upgrade to **Image Builder v0.1.45 or later**, which enforces explicit specification of Windows credentials via:
  - The WINDOWS_ADMIN_PASSWORD environment variable, or
  - The admin_password JSON parameter.
- **Rebuild and Redeploy Affected Images:**
  Rebuild Windows images using the patched version and redeploy to all nodes. Ensure the images do not contain any default or weak credentials.

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/kubernetes/issues/133115