مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Kubernetes Image Builder

Tracking #:432316424
Date:22-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Kubernetes Image Builder that could be exploited to grant unauthorized root access to the affected VMs. This could potentially lead to data exfiltration, system compromise, or denial-of-service (DoS) attacks.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the Kubernetes Image Builder, which may allow unauthorized SSH access to virtual machines (VMs) created with this tool. The flaw, tracked as **CVE-2024-9486**, affects VM images built using the Proxmox provider with Kubernetes Image Builder version **0.1.37** or earlier. This vulnerability arises from default credentials being enabled during the image-building process and not being disabled afterward, enabling attackers to gain root access via SSH. Additionally, a related vulnerability, **CVE-2024-9594**, affects images built with Nutanix, OVA, QEMU, or raw providers but has a lower severity rating due to additional exploitation requirements.

- **Critical Severity (CVSS 9.8)**: Proxmox provider (CVE-2024-9486).
- **Medium Severity (CVSS 6.3)**: Nutanix, OVA, QEMU, or raw providers (CVE-2024-9594).

The vulnerabilities allow attackers to connect to VMs using default SSH credentials that remain active post-build. For CVE-2024-9594, exploitation is limited to the build process itself and requires access to the image-creating VM.

Affected Versions:

- Kubernetes Image Builder version 0.1.37 or earlier.

Fixed Versions:

- Kubernetes Image Builder version 0.1.38 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://discuss.kubernetes.io/t/security-advisory-cve-2024-9486-and-cve-2024-9594-vm-images-built-with-kubernetes-image-builder-use-default-credentials/30119