Security Advisory 2024-112

Critical Vulnerability in Kubernetes

2024-10-17 — v1.0

TLP:CLEAR

History:

- *17/10/2024 — v1.0 – Initial publication*

Summary

On October 14, 2024, Kubernetes released a security advisory addressing a critical vulnerability affecting the Kubernetes Image Builder project [1,2].

It is recommended updating the Kubernetes Image Builder, and redeploying or mitigating Virtual Machines (VMs) created by the vulnerable Kubernetes Image Builder.

Technical Details

The flaw affects Kubernetes Image Builder version 0.1.37 and earlier. It enables root access via SSH using default credentials on VMs built with the vulnerable version of Kubernetes Image Builder [2].

For images built with the Proxmox provider, the vulnerability has been assigned `CVE-2024-9486`, with a CVSS score of 9.8.

For images built with the Nutanix, OVA, QEMU or raw providers, the vulnerability has been assigned `CVE-2024-9594`, with a CVSS of 6.3.

Affected Products

This flaw affects:

- Kubernetes Image Builder v0.1.37 and earlier;
- VM images built the vulnerable version of Kubernetes Image Builder.

Recommendations

It is strongly recommended updating the Kubernetes Image Builder and redeploying VMs created by the vulnerable Kubernetes Image Builder.

Mitigations

It is possible to mitigate the vulnerability in affected VMs by disabling the `builder` account: `usermod -L builder`

Detection

The Linux command `last builder` can be used to view logins to the affected `builder` account.

References

[1] https://www.bleepingcomputer.com/news/security/critical-kubernetes-image-builder-flaw-gives-ssh-root-access-to-vms/

[2] 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