Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Kubernetes Image Builder Flaws Could Lead VM Compromise

Date of Publication	Admiralty Code	TA Number
October 17, 2024	A1	TA2024398

Summary

First Seen: October 15, 2024
Affected Product: Kubernetes Image Builder
Impact: Two vulnerabilities have been discovered in Kubernetes environments that use the Image Builder tool to create VM images for cluster setup. One of these, identified CVE-2024-9486, allows attackers to exploit default SSH credentials in Proxmox-based VM images, leading to root access and full system compromise. The other, CVE-2024-9594, requires access during the image build process and enables persistence of default credentials. To mitigate these risks, users should upgrade to Image Builder v0.1.38 or manually disable default builder accounts.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-9486	Kubernetes Image Builder Hardcoded Credential Vulnerability	Kubernetes Image Builder	✗	✗	✓
CVE-2024-9594	Kubernetes Image Builder Hardcoded Credential Vulnerability	Kubernetes Image Builder	✗	✗	✓

Vulnerability Details

#1

Two recently disclosed vulnerabilities, CVE-2024-9486 and CVE-2024-9594, affect Kubernetes environments that use the Image Builder tool to create VM images for cluster setup. Image Builder is a critical component in automating the deployment of virtual machine images across cloud and on-premise infrastructure, making it widely used in Kubernetes and cloud-native environments.

#2

CVE-2024-9486 is a critical vulnerability that affects VM images created with the Proxmox provider in Kubernetes Image Builder versions 0.1.37 and earlier. The flaw involves default SSH credentials that are not disabled after the image-building process. This allows attackers to exploit the known credentials and gain root access to virtual machines (VMs) built with these images. The severity of this vulnerability is high because it can lead to full system compromise, enabling unauthorized remote access to critical infrastructure. To mitigate this, users are advised to upgrade to Image Builder version 0.1.38, which introduces random password generation and disables the default "builder" account

#3

CVE-2024-9594, while also serious, has a slightly lower impact rating. It affects images built with other providers such as Nutanix, OVA, QEMU, or raw providers but only under specific conditions where an attacker can access the VM during the image build process. If successful, the attacker could modify the image to persist default credentials, allowing unauthorized access later. While this flaw poses a risk, it is less likely to be exploited compared to CVE-2024-9486, as it requires physical or remote access during a specific window of time.

#4

The risks posed by these vulnerabilities are significant, especially for environments using the affected VM providers, as attackers could potentially take over key infrastructure components. Kubernetes is widely used for automating application deployment and scaling, making these vulnerabilities a concern for organizations that rely on Kubernetes clusters in production environments

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9486	Kubernetes Image Builder versions v0.1.37 and prior	cpe:2.3:a:kubernetes-sigs:image-builder:*:*:*:*:*:*:*:*	CWE-798
CVE-2024-9594	Kubernetes Image Builder versions v0.1.37 and prior	cpe:2.3:a:kubernetes-sigs:image-builder:*:*:*:*:*:*:*:*	CWE-798

Recommendations

Immediate Upgrades: Upgrade Kubernetes Image Builder to version 0.1.38 or later. This version automatically generates random passwords during the image creation process and disables the default "builder" account. This prevents attackers from exploiting the default credentials present in earlier versions.

Rebuild Affected VM Images: Rebuild any virtual machines that were created with versions prior to 0.1.38. Simply upgrading the software does not retroactively fix the default credentials issue in already deployed images. Ensure that all images created with older versions are recompiled and redeployed.

Manually Disable Default Accounts: For environments unable to upgrade immediately, manually disabling the default "builder" account can serve as a temporary solution. Using system commands to lock or disable the account will reduce unauthorized access risks while you prepare for a complete rebuild of affected virtual machines. This temporary mitigation, however, does not replace the need for the upgrade.

Implement Strong Access Controls: Review and enhance access control policies for your Kubernetes environment, ensuring that only authorized personnel have access to sensitive systems. Strong access controls limit the attack surface and reduce the likelihood of unauthorized access.

Conduct Regular Security Audits: Schedule regular security audits of your Kubernetes environment, focusing on credential management and access logs. Continuous monitoring helps identify potential vulnerabilities early and ensures compliance with security best practices.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0004 Privilege Escalation	TA0042 Resource Development
TA0006 Credential Access	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1078 Valid Accounts
T1588 Obtain Capabilities	T1588.005 Exploits	T1552.001 Credentials In Files	T1552 Unsecured Credentials

Patch Details

Upgrades to Kubernetes Image Builder version 0.1.38 or later.

Link:
https://github.com/kubernetes-sigs/image-builder/releases

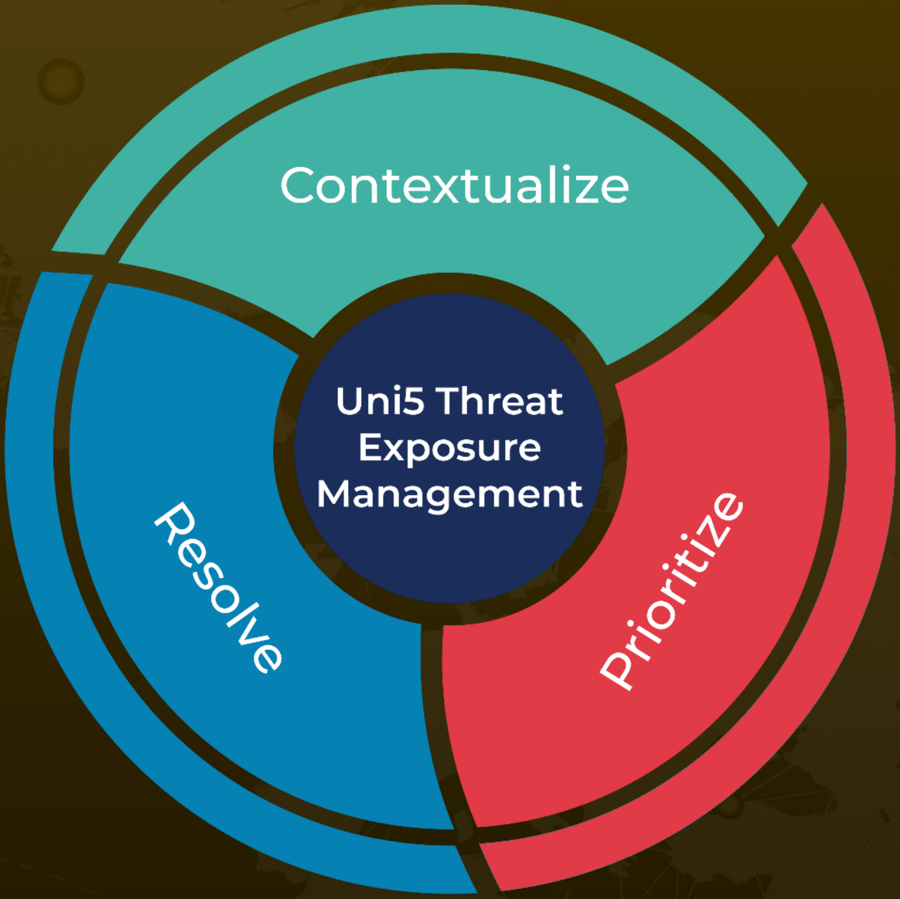
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 17, 2024 • 5:30 AM

More at www.hivepro.com