BLACKSWAN CYBERSECURITY

THREAT ADVISORY

August 20, 2024

Critical Kubernetes Flaw Exposes Clusters to Command Injection Attacks

SUMMARY

A critical Kubernetes vulnerability allows attackers to execute command injection attacks, affecting default installations across major platforms like Amazon EKS, Azure AKS, and Google GKE. The vulnerability enables malicious command execution and data exfiltration. Despite the severity, no CVE has been assigned, and an official patch is yet to be released.

VULNERABILITY DETAILS

Akamai identified the flaw, found in the git-sync project, a sidecar container within Kubernetes used to synchronize a pod with a Git repository. The issue stems from inadequate input sanitization during the synchronization process, inadvertently creating a large attack surface.

Attackers can exploit this flaw by deploying a malicious YAML file to the Kubernetes cluster, a low-privilege operation that can lead to command injection. Two parameters, GITSYNC_GIT and GITSYNC_PASSWORD_FILE, are particularly vulnerable. GITSYNC_GIT can be manipulated to replace legitimate commands with a malicious binary, allowing arbitrary code execution. Similarly, GITSYNC_PASSWORD_FILE can be used to exfiltrate sensitive information, such as access tokens, from the pod.

The consequences of this vulnerability are severe, including unauthorized command execution, data theft, and potential compromise of the entire Kubernetes cluster. Attackers could also deploy cryptominers or other malicious binaries under the guise of legitimate operations, bypassing security measures and facilitating stealthy attacks. The flaw is especially concerning for organizations with pre-authorized git-sync communication within their clusters, as attackers with minimal privileges could exploit it to gain significant control.

RECOMMENDATIONS

- Enhance monitoring of outgoing communications from Kubernetes pods, particularly those using git-sync.
- Perform regular audits of git-sync pods should be conducted to ensure they are executing only expected commands.
- Implement Open Policy Agent (OPA) rules to detect and block potential attack vectors by identifying unauthorized changes to git-sync configurations.
- Restrict editing privileges to minimize the attack surface.

REFERENCES

- https://cybersecuritynews.com/unlock-kubernetes-deployment-efficiency/
- https://www.akamai.com/blog/security-research/2024/aug/2024-august-kubernetes-gitsync-command-injection-defcon