UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00197

AZURESCAPE CROSS-CONTAINER COMPROMISE

DATE ISSUED: 13th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Exploitation of a daisy-chain of known Kubernetes vulnerabilities may allow for cross-container compromise in Azure Cloud Containers meaning attackers may be able to infiltrate other customer's containers.

BREAKDOWN

Researchers have discovered an issue in Microsoft's Container-as-a-Service (CaaS) offering in Microsoft's Azure Container Instances (ACI) allowing threat actors to gain full access to other user's containers in the multitenant Kubernetes clusters (part of the hosted infrastructure). This may lead to abuse such as resource theft for cryptomining, exfiltration of sensitive data and copying or theft of images deployed on the platform. Boundaries are enforced between containers through the underlying structure by deploying each container in a Kubernetes pod and hosting the Virtual Machines (VMs) on a dedicated, single-tenant node. In the Azurescape attacks the attacker must create and escape their own container by exploiting one of two known RunC container-escape bugs. They then attempt to gain control over the API server by obtaining a privileged Kubernetes service account token (and then the entire cluster) by executing VM commands over the "az container" dedicated bridge pod. Control over many containers is then possible as the API server acts as the front end and processes commands within each node through its interactions with Kubelets, which are the primary node agent for each specific node.

REMEDIATION STEPS

- Apply patches provided by Microsoft immediately and keep cluster infrastructure patched.
- Revoke any privileges access credentials that were deployed prior to August 31st to avoid compromise.
- Review access logs for anomalous login and behaviours or any other irregularities. Review policies regularly and monitor cluster activities.
- Enable the "BoundServiceAccountTokenVolume" feature
- Refrain from sending privileges service account token anywhere other than the API server

REFERENCES & RESOURCES

Palo Alto https://unit42.paloaltonetworks.com/azure-container-instances/
Threatpost https://threatpost.com/azurescape-kubernetes-attack-container-cloud-compromise/169319/