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

CYBER GUIDANCE ISSUE 00132

AZURE FUNCTIONS ALLOW PRIVIELEGE ESCALATION

DATE ISSUED: 12th April 2021

OVERVIEW

Users could potentially "escape" a cloud container and achieve privilege escalation by exploiting a weakness in Azure Functions known as a Royal Flush.

BREAKDOWN

The name harkens to a flush-to-disk limitation an exploit could potentially circumvent when flushing to disk hands off data to the kernel where it becomes visible to other processes. Intezer found that containers run with the privileged Docker flag allowing files in the /dev directory to be shared between the container guest and the Docker host, as these device files have "others" permissions for read-write access. Although this is not a standard behaviour, in instance where containers are affected, the Azure Functions environment has 52 partitions, with their own files systems that could become exposed. Attackers only require low-privilege user access to carry out this attack.

REMEDIATION STEPS

- Check configuration and status in your environment for known vulnerabilities and apply patches and fixes where available.
- Harden cloud environments to decrease the likelihood of a successful attack by increasing the difficulty and inconvenience for access to vulnerabilities.
- Implement runtime protections that are able to detect and respond to exploitation or in-memory attacks as they occur.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/azure-functions-privilege-escalation/165307/
Intezer https://www.intezer.com/blog/cloud-security/royal-flush-privilege-escalation-vulnerability-in-azure-functions/
Toolbox Security https://www.toolbox.com/security/cloud-security/news/privilege-escalation-flaw-discovered-in-microsofts-azure-functions/