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

CYBER GUIDANCE ISSUE 00048

AZURE APP SERVER-SIDE FORGERY REQUEST

DATE ISSUED: 12th October 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

App Services - the Microsoft Azure's HTTP-based web hosting application has recently been discovered to have two flaws that could allow attackers to gain full access and control over administration servers, particularly those running Linux.

BREAKDOWN

Available on both Microsoft Azure Cloud and on-premise, Linux-based servers are susceptible to an attack that combines two vulnerabilities to allow Server-Side Forgery Requests (SSFRs) to be executed on the Azure App Service and seize control of the system. An open source project known as KuduLite that manages the administration and registration of admins into the App Service Plan. Using the associated SSH hardcoded credentials to access the application node as root user. Thereafter malicious code may be added to the repository to spread to other instances and achiever persistence. The second flaw is a result of the KuduLite API being able to receive requests without the need for validation. A 'get' requests may be forged to access the node's file system to exfiltrate any assets on the application node including source code. A 'post' request may be used for Remote Code Execution (RCE) via the same API. When executed in combination, these two may allow full system takeover or the injection of malicious or phishing web pages.

REMEDIATION STEPS

- Install fix available from Microsoft
- Implement cloud security solutions to detect and restrict malicious activities during runtime.
- Check current cloud instance configuration to avoid misconfiguration security vulnerabilities.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/microsoft-azure-flaws-servers-takeover/159965/
Cyber Security News https://thecybersecurity.news/vulnerabilities/microsoft-azure-flaws-open-admin-servers-to-takeover-2374/
The Hacker News https://thehackernews.com/2020/10/microsoft-azure-vulnerability.html