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

CYBER GUIDANCE ISSUE 0267

MS AZURE SERVICES VULNERABILITY ALLOWS RCE

DATE ISSUED: 23rd January 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Ermetic threat researchers discovered a vulnerability in Azure cloud services knows as EmojiDeploy which allows threat actors to perform Remote Code Execution (RCE) and gain full control of the targeted machine.

BREAKDOWN

EmojiDeploy is exploited using a Cross-Site Request Forgery (CSRF) which allows an attacker to bypass the security controls in place by issuing a request to deliver a malicious archive and gain remote access. CSRF is a social engineering attack that tricks a user to execute unwanted actions on a web application in which they are currently authenticated. The Azure services which deploy Source Control Management (SCM) by default such as App Service, Function Apps. and Logic Apps are affected. It allows attackers to deploy harmful ZIP files containing malicious payloads to the Azure applications of their victims. An exploit of EmojiDeploy allows an attacker to gain full control of the machine allowing them to conduct phishing campaigns, theft or deletion of sensitive data, takeover the app's managed identity or achieve lateral movement to the Azure services. The scope of the impact is decided by the permissions on the compromised managed identity. Although the Microsoft Security Response Center (MSRC) took quick action to resolve the vulnerability, preventive measures must be taken to mitigate the effect against vulnerabilities like this in the future.

REMEDIATION STEPS

- Educate users on social engineering and the dangers of phishing attacks, how to spot them, and what to do if they receive a suspicious email in your organisation.
- Effectively applying the principle of least privilege can limit the radius of exploitation.
- Create strong and unique passwords and enable multi-factor authentication (MFA).

REFERENCES & RESOURCES

Security Boulevard https://securityboulevard.com/2023/01/emojideploy-smile-your-azure-web-service-just-got-rced-_/
The Hacker News https://thehackernews.com/2023/01/new-microsoft-azure-vulnerability.html