UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0316

MICROSOFT API MANAGEMENT FLAW

DATE ISSUED: 8th May 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

The Ermetic research team recently discovered three vulnerabilities in the Azure API Management service. These included two Server-Side Request Forgery (SSRF) vulnerabilities and a file upload path traversal on an internal Azure workload.

BREAKDOWN

The Azure API Management is platform-as-a-service (PaaS) designed to let companies develop and securely manage APIs across hybrid and multi-cloud computing environments. Microsoft has patched three new vulnerabilities in the Azure API Management service, including two Server-Side Request Forgery (SSRF) vulnerabilities and a file upload path traversal on an internal Azure workload. The vulnerabilities are a result of URL formatting bypasses and an unrestricted file upload functionality in the API Management developer portal. SSRF is a vulnerability that allows an attacker to send a crafted request from a vulnerable server to a targeted external or internal server or service. An attacker could send requests from the service's CORS Proxy and the hosting proxy itself, access internal Azure assets, deny service and bypass web application firewalls. It could result in the loss of information confidentiality and integrity, permitting a threat actor to read internal Azure resources and execute unauthorised code. Microsoft has patched all three flaws.

REMEDIATION STEPS

- Apply all recent security patches provided by Microsoft and implement recommended hardening controls.
- Several protective measures are possible at the Application and Network layers. Applying the defence-in-depth principle will harden both layers against such attacks.
- Install and regularly update your Next Generation Firewall (NGF) to limit the application's access and, in turn, limit the impact of an application vulnerable to SSRF.
- Leverage network segmentation to block illegitimate calls directly at the network level.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Hacker News	https://thehackernews.com/2023/05/researchers-discover-3-vulnerabilities.html
OWASP	https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html