مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Microsoft Power Pages

Tracking #:432316902

Date: 25-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in Microsoft Power Pages that has been actively exploited in the wild.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE ID: **CVE-2025-24989**
- Vulnerability Type: Elevation of Privilege (EoP)
- Weakness: CWE-284 (Improper Access Control)
- Max Severity: Critical
- CVSS Score: 8.2
- This vulnerability stems from improper access control (CWE-284), potentially enabling attackers to bypass user registration controls and gain unauthorized access to sensitive systems or data. The vulnerability has been assigned a CVSS score of 8.2 (Critical) due to its high impact on integrity and low impact on confidentiality.

Mitigation:

Microsoft has already mitigated this vulnerability in their service and notified all affected customers. The update addresses the registration control bypass, and customers have been provided with instructions to review their sites for potential exploitation and cleanup.

RECOMMENDATIONS:

- Apply Updates: Ensure Microsoft Power Pages environment is updated to the latest version that includes the official fix for this vulnerability.
- Review Access Controls: Conduct a thorough review of user registration controls and access permissions within your Power Pages sites to ensure no unauthorized changes have been made.
- Monitor for Exploitation: Investigate logs and user activity for signs of potential exploitation, such as unexpected privilege escalations or unauthorized access attempts

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24989