

**HiveForce Labs**

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Microsoft Fixes Power Pages Critical Flaw Exploited in Active Attacks

Date of Publication

February 24, 2025

Admiralty Code

A1

TA Number

TA2025056




# Summary

**First Seen:** February 19, 2025

**Affected Products:** Microsoft Power Pages

**Impact:** Microsoft has patched a critical vulnerability, CVE-2025-24989, in Power Pages, which was actively exploited in attacks. This flaw stems from improper access controls, allowing attackers to escalate privileges over a network and bypass user registration restrictions. Since hackers have already been exploiting this vulnerability, organizations using Power Pages should apply the fix immediately to prevent unauthorized access.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24989	Microsoft Power Pages Improper Access Control Vulnerability	Microsoft Power Pages			

# Vulnerability Details

## #1

Microsoft has addressed a critical flaw, CVE-2025-24989, in Power Pages, a platform designed for building and managing external-facing business websites. This flaw, caused by improper access controls, allowed attackers to bypass user registration mechanisms and escalate privileges, potentially gaining unauthorized control over affected sites. The vulnerability has been actively exploited in the wild, raising concerns about potential unauthorized access to sensitive data.

## #2

The issue is mitigated at the service level and notified impacted users with remediation steps. Organizations using Power Pages should audit their environments for unauthorized accounts, privilege escalations, or unusual access patterns.

## #3

If any suspicious activity is detected, immediate action should be taken to revoke unauthorized accounts, reset affected credentials, and enforce multi-factor authentication (MFA) to strengthen security. Even if no direct notification was received, it is recommended to apply security best practices, including regularly reviewing access logs and updating permissions, to prevent similar attacks in the future.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24989	Microsoft Power Pages	cpe:2.3:a:microsoft:power_pages:*.:*:*:*:*:*	CWE-284

## Recommendations



**Stay Updated:** Make sure all Power Pages instances are running the latest security patches. Stay vigilant by regularly checking Microsoft security advisories for new updates and applying them promptly.



**Review Activity Log:** Regularly review activity logs to detect unauthorized access or privilege escalations. Investigate and respond to any suspicious activity promptly. Turn on logging and auditing to monitor user actions on Power Pages. Look into any unexpected access attempts or unauthorized privilege escalations. Look for any unauthorized accounts or unusual activity.



**Restrict User Privileges:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



**Strengthen Security with Multi-Factor Authentication (MFA):** Activate MFA on all accounts to enhance security and prevent unauthorized access. Ensure that administrators use strong authentication methods for added protection.



**Implement Web Application Firewall (WAF):** Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit vulnerability, providing an additional layer of protection.

## Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0001</b> Initial Access	<b>TA0004</b> Privilege Escalation	<b>T1588</b> Obtain Capabilities
<b>T1588.006</b> Vulnerabilities	<b>T1190</b> Exploit Public-Facing Application	<b>T1068</b> Exploitation for Privilege Escalation	

## Patch Details

Microsoft has patched CVE-2025-24989 in Power Pages with a service-level mitigation and notified affected users. If you have not received such a notification, your deployment is likely unaffected.

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

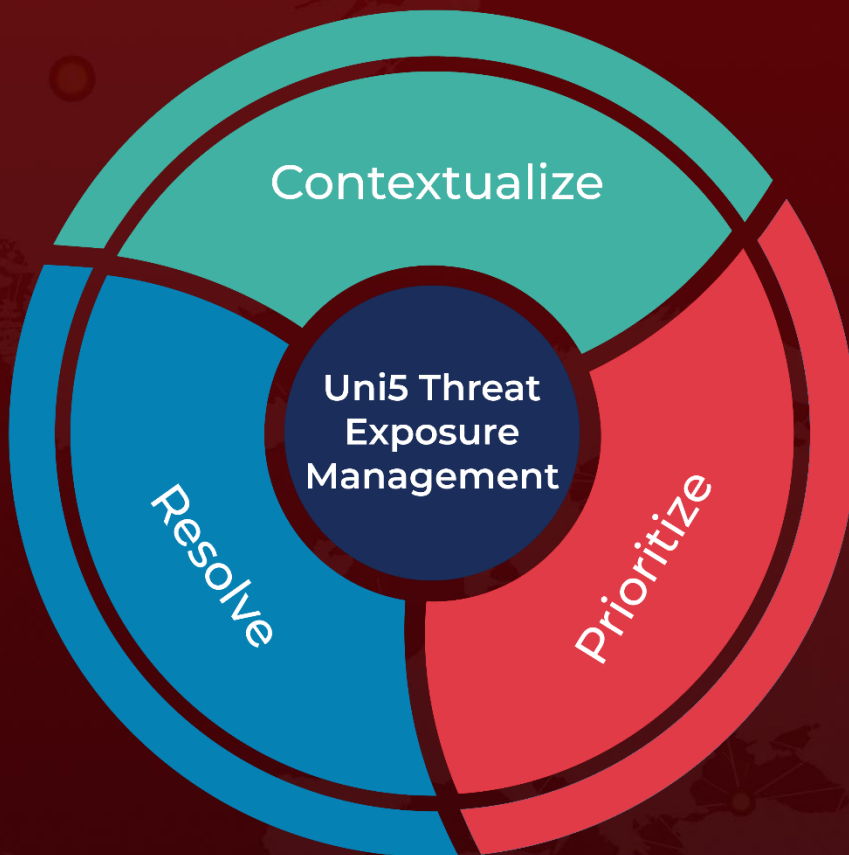
## References

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

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**February 24, 2025 • 4:00 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)