EnCyb

Severity: Critical

Advisory Type: Security

# Windows Admin Center Privilege Escalation Vulnerability

Advisory Report

TLP: WHITE

## SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

## EXECUTIVE SUMMARY

A critical elevation-of-privilege vulnerability (CVE-2026-26119, CVSS 8.8) in Windows Admin Center v2.6.4 allows low-privileged authenticated users to escalate privileges over the network due to improper authentication (CWE-287).Microsoft has released a security update, and organizations should prioritize patching immediately to reduce the risk of lateral movement and full infrastructure compromise.

- CVE: CVE-2026-26119
- CVSS: 8.8
- Active Region: Global
- Affected Sector: Enterprise IT / Organizations using centralized server management
- Affected Product: Windows Admin Center v2.6.4

  Severity: Critical
- Published Date: January 18, 2026

## TECHNICAL DETAILS

- **Target:** Systems running Windows Admin Center v2.6.4, particularly enterprise environments where WAC is exposed for centralized server, cluster, or infrastructure management. Because WAC often has broad administrative reach, compromise can impact multiple managed assets.
- **Root Cause:** Improper authentication (CWE-287) within Windows Admin Center that fails to adequately enforce privilege boundaries, enabling an authenticated user to escalate permissions beyond their intended authorization level.
- **Prerequisite For Exploitation:** The attacker must already possess low-privileged authenticated access to the WAC instance over the network. No user interaction is required, attack complexity is low, and the vulnerability can be exploited remotely if the management interface is accessible.

## IMPACT

- Privilege escalation to administrative-level access
- Full control over managed servers and infrastructure
- Lateral movement across enterprise networks
- Exposure of sensitive data and configurations
- Unauthorized modification of system and security settings
- Potential service disruption and operational impact
- Establishment of persistent unauthorized access

## RECOMMENDATIONS

- Immediately apply the latest security update for Windows Admin Center.
- Restrict network access to Windows Admin Center.
- Enforce the principle of least privilege for all administrative accounts.
- Implement multi-factor authentication (MFA) for privileged access.
- Review and audit existing user roles and permissions within WAC.
- Regularly conduct vulnerability scanning and configuration assessments.

## REFERENCE

- https://gbhackers.com/critical-flaw-in-windows-admin-center-exposes/

# SECURE, SCALE, SUCCEED WITH CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com