



BULLETIN DE SECURITE

Titre	Vulnérabilités dans Microsoft Azure (Patch Tuesday Mars 2026)
Numéro de Référence	61891103/26
Date de Publication	11 Mars 2026
Risque	Important
Impact	Important

Systemes affectés

- Azure Automation Hybrid Worker Windows Extension;
- Azure MCP Server Tools;
- Arc Enabled Servers - Azure Connected Machine Agent;
- Azure Linux Virtual Machines with Azure Diagnostics extension;
- Azure IoT Explorer;
- Microsoft Azure AD SSH Login extension for Linux;
- Windows Admin Center in Azure Portal ;

Identificateurs externes

- CVE-2026-26141 CVE-2026-26118 CVE-2026-26117 CVE-2026-23665 CVE-2026-23662
- CVE-2026-23661 CVE-2026-26148 CVE-2026-26121 CVE-2026-23664 CVE-2026-23660

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Azure susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant d'élever ses privilèges, de divulguer des informations sensibles ou encore de réussir une usurpation d'identité.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 10 Mars 2026.

Risque

- Élévation des privilèges ;

- Divulcation d'informations confidentielles ;
- Usurpation d'identité ;

Annexe

Bulletin de sécurité Microsoft du 10 Mars 2026:

- <https://msrc.microsoft.com/update-guide/>