DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 05-11-2025

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans les produits Azure Access Technology
Réference	1413
Date de Publication	2025-11-02
Sévérité	Critique

IMPACT :

- Déni de service ;
- Exfiltration de données sensibles ;

SYSTÉME AFFECTÉ :

- Azure Access Technology BLU-IC2
- Azure Access Technology BLU-IC4

DÉSCRIPTION :

Trois vulnérabilités critiques ont été identifiées dans les produits Azure Access Technology « BLU-IC2 et BLU-IC4 », susceptibles d'entraîner un déni de service, des compromissions de communication, ou des accès non autorisés.

CONTOURNEMENT PROVISOIRE :

Aucune mise à jour corrective n’est actuellement disponible. Des mesures de mitigation immédiates sont fortement recommandées.

- Restreindre l’accès aux interfaces API aux seules adresses IP de confiance.
- Mettre en place un filtrage d’entrée strict sur les paramètres de localisation.
- Réduire les timeouts des connexions HTTP/TCP.
- Activer la limitation du nombre de connexions simultanées.
- Mettre en place une surveillance réseau active pour détecter les attaques lentes.
- Restreindre l’accès au port TCP/5000 aux réseaux internes de confiance uniquement.
- Segmenter le réseau pour isoler les dispositifs BLU-IC2/IC4.
- Mettre en œuvre un chiffrement réseau additionnel (VPN/IPSec).
- Surveiller les logs applicatifs pour détecter toute activité suspecte

DOCUMENTATION :

Bulletin de sécurité Azure Access Technology :

- https://azure-access.com/security-advisories/