Avertissement de sécurité lors de la connexion à Gestan Cloud via rdp (avril 2026)

Contexte

Depuis la mise à jour de sécurité Windows d'avril 2026 (KB5083769 pour Windows 11, KB5082052 pour Windows 10), Microsoft a renforcé la sécurité du client Bureau à distance (RDP). De nouveaux avertissements de sécurité s'affichent désormais lors de l'ouverture d'un fichier de connexion `.rdp` ou du lancement d'un programme RemoteApp.

Cette mesure vise à protéger les utilisateurs contre les tentatives de phishing utilisant des fichiers `.rdp` malveillants. Des acteurs malveillants (notamment le groupe russe APT29/Midnight Blizzard) utilisaient ce type de fichiers pour rediriger silencieusement les ressources locales des victimes (presse-papiers, lecteurs, caméra…) vers des serveurs contrôlés par des pirates.

Cette modification, déployée sans préavis par Microsoft, a pris de court l'ensemble des éditeurs de solutions utilisant la technologie Bureau à distance. Gestan Cloud est concerné au même titre que de très nombreuses autres solutions professionnelles s'appuyant sur le protocole RDP.

Votre connexion à Gestan Cloud n'est pas affectée et reste parfaitement sécurisée. Il s'agit d'étapes de vérification supplémentaires introduites par Microsoft.

Les deux avertissements expliqués

La mise à jour introduit en réalité **deux fenêtres distinctes** qu'il est important de ne pas confondre.

1. Le message éducatif (une seule fois)

Lors de votre **toute première connexion** après installation de la mise à jour, une fenêtre éducative de Microsoft apparaît. Elle vous explique ce que sont les fichiers de connexion à distance et les risques potentiels liés au phishing. Ce message n'apparaît **qu'une seule fois** par compte utilisateur Windows : il vous suffit de cliquer sur **OK** pour le valider. Il ne reviendra plus par la suite.

2. Le dialogue de sécurité de connexion (à chaque lancement)

À chaque lancement de Gestan Cloud, une fenêtre intitulée **« Avertissement de sécurité RemoteApp »** s'affiche avec le bandeau **« Attention : connexion distante inconnue »**. C'est le comportement normal et attendu depuis la mise à jour.

Cette fenêtre affiche les informations suivantes :

- **Éditeur** : Serveur de publication inconnu
- **Type** : Programme RemoteApp
- **Ordinateur distant** : cloudX.gestan.fr (où X correspond au numéro de votre serveur, par exemple cloud8.gestan.fr)
- **Nom de RemoteApp** : RemoteApp
- **Chemin RemoteApp** : logonsession

En dessous, une liste de ressources locales que la connexion demande à partager avec le serveur distant apparaît avec des cases à cocher, **toutes décochées par défaut**.

Que faire à chaque connexion ?

Étape 1 — Vérifiez que l'adresse de l'ordinateur distant correspond bien à un serveur Gestan Cloud. L'adresse doit être de la forme `cloudX.gestan.fr` (par exemple cloud8.gestan.fr). Si vous voyez une adresse que vous ne reconnaissez pas, ne poursuivez pas et contactez notre support.

Étape 2 — **Cochez toutes les cases** de la liste des ressources locales. C'est important : les cases étant décochées par défaut depuis la mise à jour, si vous ne les activez pas, vos disques locaux, vos imprimantes, votre presse-papiers et vos autres périphériques ne seront pas partagés avec la session Gestan Cloud. Concrètement, cela signifie que vous ne pourrez pas imprimer depuis Gestan, ni faire de copier-coller, ni accéder à vos fichiers locaux pour les imports/exports.

Étape 3 — Cliquez sur **« Connexion »** pour lancer Gestan Cloud.

Cette vérification ne prend que quelques secondes et deviendra un réflexe après quelques utilisations.

Pourquoi l'éditeur s'affiche-t-il comme « inconnu » ?

L'avertissement indique « Serveur de publication inconnu » car le fichier de connexion utilisé par le connecteur Gestan Cloud n'est pas encore signé numériquement par un certificat reconnu par Microsoft. C'est un comportement attendu pour la très grande majorité des solutions de connexion à distance tierces : elles ont toutes été prises de court par cette mise à jour. Les fichiers RDP signés (comme ceux d'Azure Virtual Desktop ou Windows 365) affichent l'identité de l'éditeur à la place du message d'alerte, mais la plupart des solutions professionnelles ne disposent pas encore de ce type de signature.

Cela ne remet pas en cause la sécurité de votre connexion. Nos serveurs cloud restent sécurisés et surveillés comme d'habitude.

Pourquoi cet avertissement revient-il à chaque fois ?

Contrairement au premier message éducatif qui n'apparaît qu'une seule fois, le dialogue de sécurité de connexion s'affiche **à chaque ouverture d'un fichier .rdp**. C'est un choix délibéré de Microsoft : cette fenêtre a pour but de vous permettre de vérifier systématiquement l'adresse du serveur distant et de contrôler quelles ressources locales vous partagez, avant que la connexion ne soit établie.

C'est comparable à la fenêtre de confirmation qui apparaît lorsque vous autorisez une application à accéder à votre position ou votre microphone sur un smartphone : il s'agit de vous donner le contrôle à chaque fois.

Et la suite ?

Nous travaillons d'ores et déjà à la **signature numérique du connecteur Gestan Cloud**. Une fois cette signature en place, la mention « Serveur de publication inconnu » sera remplacée par l'identité vérifiée de l'éditeur, et l'expérience de connexion sera simplifiée.

Nous vous tiendrons informés dès que cette évolution sera disponible. En attendant, l'étape de vérification décrite ci-dessus reste nécessaire à chaque connexion via le connecteur RDP, ou vous pouvez utiliser l'accès par navigateur web décrit plus haut.

En savoir plus

Pour plus d'informations techniques sur cette modification apportée par Microsoft, vous pouvez consulter la documentation officielle : Understanding security warnings when opening Remote Desktop (RDP) files (en anglais).

Si vous rencontrez la moindre difficulté, n'hésitez pas à contacter notre support technique.