



## BULLETIN DE SECURITE

|                            |   |
|----------------------------|---|
| <b>Titre</b>               | Vulnérabilité critique au niveau du ECM Hyland OnBase |
| <b>Numéro de Référence</b> | 61131602/25   |
| <b>Date de Publication</b> | 16 Février 2026                                       |
| <b>Risque</b>              | Critique  |
| <b>Impact</b>              | Critique  |

### Systèmes affectés

- Hyland OnBase – Workflow Timer Service (Hyland.Core.Workflow.NTService.exe);
- Hyland OnBase – WorkView Timer Service ;

### Identificateurs externes

- CVE-2026-26221 ;

### Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans les versions susmentionnées du ECM "Hyland OnBase". Cette faille peut permettre à un attaquant d'envoyer des requêtes spécialement conçues via le port TCP 8900, afin de lire et écrire des fichiers arbitraires sur le système et d'exécuter du code arbitraire à distance, ainsi de contourner la politique de sécurité.

L'attaquant peut aussi utiliser un chemin « UNC » malveillant pour forcer le système cible à s'authentifier à un serveur malveillant. Ce processus expose les informations d'authentification (hachages NTLM) que l'attaquant peut ensuite exploiter pour accéder à des ressources réseau ou effectuer un relai NTLM.

### Solution

Veuillez se référer au bulletin de sécurité Hyland OnBase du 13 Février 2026 pour plus d'information.

### Risque

- Exécution des commandes arbitraires à distance ;
- Atteinte à la confidentialité des données ;
- Atteinte à l'intégrité des données ;
- Contournement de la politique de sécurité ;

## Annexe

Bulletin de sécurité Hyland OnBase du 13 Février 2026:

- <https://www.hyland.com/en/solutions/products/onbase>