



BULLETIN DE SECURITE

| | |
|----------------------------|---|
| Titre | Vulnérabilités critiques dans Trend Micro Apex Central (on-premise) |
| Numéro de Référence | 59851201/26 |
| Date de Publication | 12 Janvier 2026 |
| Risque | Critique |
| Impact | Critique |

Systèmes affectés

- Trend Micro Apex Central (on-premise) Version antérieure à Critical Patch Build 7190,

Identificateurs externes

- CVE-2025-69258, CVE-2025-69259, CVE-2025-69260,

Bilan de la vulnérabilité

Trend Micro a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités affectant Apex Central (versions on-premise Windows). La vulnérabilité la plus grave, CVE-2025-69258 (CVSS 9.8), permet à un attaquant distant non authentifié de charger une bibliothèque DLL malveillante sur le serveur Apex Central. Cette action peut entraîner l'exécution de code arbitraire avec des droits SYSTEM via le composant MsgReceiver.exe.

Deux autres vulnérabilités, CVE-2025-69259 et CVE-2025-69260, permettent de provoquer un déni de service à distance. Elles exploitent également le composant MsgReceiver.exe, accessible par défaut sur le port TCP 20001.

Solution :

- Appliquer les correctifs Trend Micro et mettre à jour vers Build 7190 ou supérieur.
- Restreindre l'accès réseau au port 20001.
- Surveiller toute activité anormale liée à MsgReceiver.exe.

Risque :

- Exécution du code à distance ;
- Déni de service ;

Annexe

Bulletin de sécurité Trend Micro du 09 Janvier 2026:

- <https://success.trendmicro.com/en-US/solution/KA-0022071>