



Un point sur la sécurité 2025/2026

Introduction

- L'IBM i est un des systèmes les plus sûrs du marché



Introduction

- Mais c'est souvent l'un des moins bien protégé



Les causes...

- Méconnaissances des principes de Sécurité de l'IBM i
- Développeurs et éditeurs de logiciels
- Applications anciennes qui datent d'une époque où il n'y avait pas ou peu de réseau, pas de hackers, pas de ransomware...
- Dérive de la configuration originelle
- Et pourtant les IBM i sont critiques et contiennent des informations et des programmes vitaux pour vos structures

2024-2025

- Forte recrudescence des attaques utilisant des informations **d'identifications valides**
 - L'utilisation de comptes valides est devenue le point d'entrée le plus courant des cybercriminels
 - C'est beaucoup, beaucoup plus difficile à détecter !
 - Et on les aide beaucoup !
- Le **vol de données** est en forte progression. De plus en plus de groupes privilégient cette méthode pour obtenir des gains financiers
- Rançon : pour mémoire de l'ordre de 10 % du Chiffre d'Affaires annuel

2025/2026

- Toujours utilisation des informations **d'identifications valides**
- Le vol de données (exfiltration) se confirme
- L'IA de pointe a radicalement transformé le paysage des cybermenaces
 - À la fois coté attaquant
 - Et défenseur

Menaces liées aux identifiants

- Le vol d'identifiants devance désormais l'exploitation des failles de sécurité et constitue le point d'entrée majoritaire des intrusions
- Mot de passe par défaut
 - Identique au profil utilisateur
- Contraintes de mot de passe faibles
 - QPWLVL doit être à 3 ou 4 ($\geq$ V7R5)
 - Longueur, type de caractères
- Les comptes de service
 - Parfois enregistrés en clair avec le mot de passe (en local ou à distance)
 - Maîtrise des comptes de service
- Mots de passe/profil en clair dans l'IFS, partagé par NetServer
- Pas de SSL



Les attaques basées sur l'identité présentent un intérêt décisif pour les acteurs malveillants : elles permettent en effet de mener toute une série d'opérations malveillantes, souvent avec un minimum d'efforts et sans rencontrer beaucoup de résistance du point de vue de la sécurité. L'explication est simple : cette activité est difficile à détecter, parce qu'elle émane de comptes d'utilisateurs apparemment légitimes.

Menaces persistantes avancées

- Advanced Persistent Threat (APT)
- Ce sont des cyberattaques « indétectables » conçues pour voler des données sensibles, mener du cyberespionnage ou saboter des systèmes critiques sur une longue période
- Contrairement à d'autres cybermenaces comme les ransomwares, l'objectif d'un groupe d'attaques APT est de rester inaperçu tout en infiltrant et étendant sa présence au sein d'un réseau cible
- Sophistiquées et persistantes, opèrent à bas bruit
- Souvent opérées par des groupes organisés (états voyous ou des groupes criminels très bien organisés)
- Objectifs : voler des données, à recueillir des informations et à maintenir une présence invisible le plus longtemps possible

Exfiltration de données

- C'est une tendance qui se confirme
 - Voir actualité récente avec le vol de données de Impots.gouv.fr
 - Environ 700 000 comptes
- C'est plus facile à faire que de tout bloquer
 - C'est facile à revendre
- Nos IBM i ne sont pas correctement protégés en général
 - Base de données avec des droits publics élevés
 - IFS non protégé et souvent exposé (NetServer)

Détournement de session

- L'idée consiste à dérober des tokens de sessions
- Il s'agit de détourner les sessions utilisateur
 - Et parfois de rester connecté, même après un changement de mot de passe
- Plutôt que de dérober des mots de passe, les attaquants volent simplement l'état d'authentification de l'utilisateur
- Surtout pour le Cloud
 - Office 365
 - Google Workspace
 - Et autres services cloud
- Ces tokens peuvent être immédiatement revendus sur le dark web ou utilisés directement pour des intrusions

Secure Shell (SSH)

- SSH est un protocole sécurisé
 - Hérité du monde Unix
 - Ligne de commande et transfert de fichiers (SFTP)
- Sur IBM i il était surtout utilisé
 - Par les administrateurs Unix/Linux qui ont leurs habitudes avec ce protocole
 - Pour la gestion des modules Open Source
- Notre pot de miel (IBM i sur Internet dans aucune protection) nous montre que l'immense majorité des attaques est réalisée via SSH
 - Et le compte ROOT à plus de 80 %
 - Voir l'exemple à suivre de test de pénétration
- Je recommandais de laisser le serveur arrêté et de ne le démarrer que lorsqu'il y a un besoin

Secure Shell (SSH) 2

- Mais, il est nécessaire à de plus en plus de produits
- Notamment Bob
- Ce qui nous oblige à l'avoir démarré en permanence
- Il faut donc absolument le sécuriser et le tracer !



« SSH sur IBM i, c'est comme une porte dérobée dans un château médiéval : si tu laisses **QSECOFR** ou un profil *all access* se connecter en SSH... ➡ tu mérites l'invasion. »
CoPilot

Protéger Secure Shell (SSH)

- Forcer l'authentification par clés SSH (pas de mot de passe)

« Les mots de passe pour SSH sur IBM i... ➡ c'est comme protéger un château avec une corde et un panneau "ne pas entrer". »
CoPilot



- Restreindre l'environnement SSH avec *chroot* afin de contraindre ce qu'il peut faire
- Tracer (interdire) les connexions, via les points d'exit par exemple
- ...



Que fait IBM pour la sécurité IBM i ?

- Annonces régulières
 - FLASH: Security Bulletin
- Ces annonces sont généralement assorties de PTFs
- Plus de 50 flashes depuis août 2026
- Nous relayons celles qui nous paraissent importantes sur le compte LinkedIn de I.GAYTE.IT
- Nous conseillons, bien sûr, d'appliquer ces correctifs
 - ! ACS 1.1.9.14 corrige plusieurs problèmes de sécurité mais a quelques soucis (SSL)
 - Depuis la 1.1.9.15 est sortie
 - SSL OK

Par Agustin Zavala • 18/08/2026

...



i.gayte.it
365 abonnés
2 j •

Alerte de sécurité : nouveaux bulletins concernant IBM i

IBM a publié le 17 août 2026 de nouveaux bulletins de sécurité concernant IBM i.

- CVE-2026-18102 – Buffer Overflow

L'IBM i pourrait permettre à un attaquant distant authentifié d'écraser des zones mémoire adjacentes en raison d'un sous-dépassement d'entier lors de la vérification des limites.

- CVE-2026-17015 – Denial of Service dans les Host Servers

L'IBM i pourrait permettre à un attaquant distant authentifié de provoquer un déni de service et d'obtenir des informations sensibles en raison d'une lecture hors limites.

- Mesures

- Vérifier si votre version d'IBM i est concernée
- Contrôler les PTF et correctifs disponibles
- Consulter les bulletins IBM pour les détails techniques et les conditions d'exposition

Sources IBM

- CVE-2026-18102 : <https://lnkd.in/eAkPVvFe>

- CVE-2026-17015 : <https://lnkd.in/euQU6hDh>

Y'a pas de sécurité !

- IA : pas de sécurité !
- L'IA est à la fois
 - Un puissant atout pour la défense
 - Et un excellent outil pour augmenter la surface d'attaque



IBM : Cost of Data Breach 2026

- Les attaques pilotées par l'IA ont augmenté de 56 % par rapport à l'étude de l'an dernier
- Elles ont ajouté en moyenne 1 million USD au coût de chaque violation, les outils d'IA permettant aux cybercriminels d'accroître leur vitesse et leur échelle d'action. Cette rapidité redéfinit l'économie des violations, et pas dans le bon sens.



Les données que l'on confie à l'IA

- Que peuvent-elles voir ?
 - Codes source, données sensibles
- Que peuvent-elles faire ?
 - Logins, droits IBM i, lecture/écriture, approbation
- Peut-on le prouver ?
 - Journaux, versions, approbations
- IA Act
 - Depuis début août, on est tous beaucoup plus contraint
- Journée de demain consacrée à l'IA en grande partie

Merci

Dominique GAYTE – i.GAYTE.IT



info@gayte.it - <https://i.gayte.it>