Listes des partcipnts

KIDIMBA LUNZI
KALOMBO NEEMA
SHAKO ONIA
MAMPWO SEMETE
BWEMA ISAAC
MOKAMO NDOMBE
SENGI OSCA
AWASSO MAKAYA
MNAWU NZUZI
MAKUKA NGIEDI
NSILULU MAVUNGU
YAMAYAMA KIFAKIO
MALANDA TOKO
MUCHAIL KAMIN
KATSHAY MPENGO

RISQUE 1

Les Vulnérabilités non corrigées / CVE (patching manquant)

Des failles connues (CVE) dans Oracle Database / E-Business Suite / composants associés peuvent être exploitées si les correctifs ne sont pas appliqués rapidement.

Mesures / recommandations :

- Appliquer régulièrement les Critical Patch Updates Oracle et suivre les Security Alerts.
- Intégrer un processus de gestion des correctifs (test → déploiement) et scanner les environnements pour CVE.

Conséquences si exploité :

Exécution de code à distance, vol de données, chiffrement par ransomware, compromission complète du système.

Commentaire :

Maintenir une hygiène de patching est prioritaire — les attaquants exploitent souvent des failles déjà corrigées dans des systèmes non-patchés.

RISQUE 2

L'Injection SQL via applications (faiblesse côté applicatif)

Si une application en amont transmet des requêtes SQL construites dynamiquement sans paramétrage/validation, un attaquant peut exécuter des requêtes arbitraires.

Mesures / recommandations :

- Utiliser des requêtes paramétrées (bind variables), procédures stockées sécurisées et ORM bien configurés.
- Valider/sanitiser les entrées côté serveur, appliquer le principe du moindre privilège pour les comptes applicatifs.
- Déployer un pare-feu applicatif SQL (Database Firewall / SQL Firewall) et surveiller les requêtes anormales.

Conséquences si exploité :

Fuite ou modification de données, contournement d'authentification, pivot vers d'autres systèmes.

Commentaire :
La sécurité du SGBD dépend souvent de la robustesse des couches applicatives — corriger l'input handling réduit énormément le risque.

RISQUE 3

Mauvaises configurations et comptes par défaut / mots de passe faibles

listeners, services ou comptes avec mots de passe par défaut, scripts non exécutés, ou fichiers sensibles exposés.

Mesures / recommandations :

- Supprimer ou sécuriser les comptes par défaut, exiger des mots de passe forts et rotation régulière. Exécuter secconf.sql et suivre les hardening guides.
- Restreindre l'accès au listener (TNS) et désactiver les services inutiles ; protéger le port 1521 par firewall/NAC.

Conséquences si exploité :

accès non autorisé, élévation de privilèges, exfiltration de données.Commentaire : la plupart des audits retrouvent encore des installations avec paramètres par défaut — corriger ça est souvent un « gain facile » en sécurité.

RISQUE 4

Privilèges excessifs / mauvaise gestion des rôles et des comptes

Les comptes DBA trop permissifs, absence de séparation des tâches (SoD), absence de contrôle granulaire d'accès

Mesures / recommandations :

- Appliquer le principe du moindre privilège : comptes applicatifs et utilisateurs avec permissions minimales.
- Mettre en place des rôles définis, revue périodique des privilèges, séparation des tâches et approbation pour élévation de droits. Utiliser l'audit et la journalisation fine (Audit Vault, Unified Auditing).

Conséquences si exploité :

modifications non autorisées, sabotage interne, dissimulation d'activités malveillantes.

Commentaire :

la gouvernance des comptes est critique même sans faille technique, de mauvais privilèges mènent à un risque élevé.

RISQUE 5

Chiffrement / communications réseau faibles et fuite de données au repos

L'utilisation de TLS obsolète, absence de chiffrement des données sensibles au repos ou mauvaise gestion des clés.

Mesures / recommandations :

- Migrer vers TLS 1.2/1.3 et désactiver les protocoles/cipher suites obsolètes. Configurer correctement le chiffrement réseau.
- Chiffrer les données sensibles au repos (TDE – Transparent Data Encryption), gérer les clés via Oracle Key Vault ou solution KMS centralisée. Activer le masquage dynamique si nécessaire.

Conséquences si exploité :

interception de données en transit, extraction de données sensibles non protégées, non-conformité réglementaire.

Commentaire :

même si un attaquant n'accède pas directement à la base, une mauvaise protection des données rend toute compromission catastrophique.