CYBERSHIELD

Consulting | Audit | Sécurité des SI

RAPPORT D'AUDIT DE SÉCURITÉ PRÉLIMINAIRE

Evaluation de la posture de sécurité applicative
Module ERP Indus Portal - Iron4Software

Client	Iron4Software SAS
Référence	CS-2026-AUD-0847
Version	0.9 - Pré-rapport (draft)
Classification	CONFIDENTIEL
Date	12 février 2026
Auditeur principal	Marc Delacroix, CISSP, CEH
Auditeur associé	Sarah Benchetrit, OSCP
Diffusion	Direction Generale Iron4Software uniquement

CONFIDENTIEL - Ne pas diffuser sans autorisation de CyberShield Consulting

Ce document constitue un pré-rapport soumis à validation. Les conclusions finales pourront évoluer.

SOMMAIRE

1. Contexte et périmètre de l'audit

Iron4Software SAS a mandaté CyberShield Consulting pour réaliser un audit de sécurité de son application principale, **ERP Indus Portal**, solution de gestion intégrée destinée aux PME du secteur industriel. Cet audit s'inscrit dans une démarche de mise en conformité et d'amélioration continue de la sécurité du système d'information.

Le périmètre de l'audit couvre les composants suivants :

Composant	Version	Environnement
ERP Indus Portal - Backend API	4.7.2	Production / Staging
ERP Indus Portal - Frontend	4.7.2	Production
Module Facturation	2.3.1	Production
API Clients (REST)	2.1.0	Production
Infrastructure de déploiement	N/A	Azure DevOps + MinIO

2. Méthodologie

L'audit a été conduit selon la méthodologie **OWASP Testing Guide v4.2** et les référentiels ANSSI applicables. Les tests ont été réalisés en mode **grey box** : l'équipe d'audit disposait d'un accès au code source et a la documentation technique, sans accès aux environnements de production.

Les phases suivantes ont été exécutées entre le 20 janvier et le 7 février 2026 :

Phase	Description	Duree
Revue de code statique	Analyse SAST du code source (SonarQube, Semgrep)	5 jours
Tests d'intrusion applicatifs	Tests manuels et automatisés sur l'environnement de staging	4 jours
Revue de configuration	Analyse des configurations serveurs, BDD, CI/CD	3 jours
Analyse des flux de données	Cartographie des flux et vérification du chiffrement	2 jours

3. Synthese des resultats

L'audit a révélé **14 vulnérabilités** dont la répartition par criticité est la suivante :

Criticite	Nombre	Description
CRITIQUE	3	Exploitation immédiate possible, impact majeur sur la confidentialité
HAUTE	4	Exploitation probable, nécessitant une remédiation rapide
MOYENNE	5	Risque modéré, remédiation panifiable
FAIBLE	2	Risque limité, amélioration recommandée

Conclusion préliminaire : La posture de sécurité de l'application ERP Indus Portal présente des faiblesses significatives, en particulier sur la gestion des secrets applicatifs et la protection des données clients. Les 3 vulnérabilités critiques identifiées nécessitent une remédiation immédiate avant toute mise en production de la version 4.8.

Note : Ce pré-rapport présente les constats préliminaires. L'analyse forensique du module de facturation est encore en cours et pourrait révéler des vulnérabilités supplémentaires. Le rapport final sera livré le 28 février 2026.

4. Constats detailles

4.1 Gestion des secrets applicatifs

Référence	CS-2026-0847-01	Criticité	CRITIQUE
CVSS 3.1	9.1	CWE	CWE-798 (Hard-coded Credentials)

Constat : L'analyse du code source a révélé la présence de secrets applicatifs en clair dans plusieurs fichiers de configuration (.env, config.json, appsettings.json). Ces fichiers contiennent des credentials de bases de données de production, des clés API tierces (Stripe, SendGrid), des tokens d'accès Azure DevOps, et des secrets JWT.

Impact : Un attaquant ayant accès au code source ou à un poste de développeur pourrait obtenir un accès direct aux bases de données de production, aux systèmes de paiement, et à l'infrastructure CI/CD. L'impact sur la confidentialité et l'intégrité des données est maximal.

Preuve : Fichier .env a la racine du dépôt contenant 12 secrets en clair (voir Annexe A - fichier joint a ce rapport).

Recommandation : Migration immédiate vers un gestionnaire de secrets (HashiCorp Vault, Azure Key Vault). Rotation de l'ensemble des credentials compromis. Ajout de .env au .gitignore et scan pre-commit avec des outils de détection de secrets (gitleaks, trufflehog).

4.2 Sécurité des API exposées

Référence	CS-2026-0847-02	Criticité	CRITIQUE
CVSS 3.1	8.6	CWE	CWE-306 (Missing Authentication)

Constat : Plusieurs endpoints de l'API REST (/api/v2/clients/export, /api/v2/admin/config) sont accessibles sans authentification ou avec un simple token statique. L'endpoint d'export des données clients permet le téléchargement de l'intégralité de la base clients au format CSV sans contrôle d'accès granulaire.

Impact : Exfiltration massive de données clients (données personnelles, IBAN, informations contractuelles). Non-conformité RGPD caractérisée. Risque de sanction par la CNIL.

4.3 Gestion des accès et authentification

Référence	CS-2026-0847-03	**Criticité**	**HAUTE**
CVSS 3.1	7.5	**CWE**	CWE-521 (Weak Password Requirements)

Constat : La politique de mots de passe de l'Active Directory interne est insuffisante. Plusieurs comptes de service et comptes utilisateurs utilisent des mots de passe triviaux. L'absence de MFA sur les accès SSH et VPN expose l'infrastructure a des attaques par force brute.

Impact : Compromission de comptes par attaque par dictionnaire ou force brute. Mouvement latéral facilite en cas de compromission initiale.

4.4 Protection des données clients

Référence	CS-2026-0847-04	**Criticité**	**CRITIQUE**
CVSS 3.1	8.8	**CWE**	CWE-312 (Cleartext Storage of Sensitive Info)

Constat : Les données clients sensibles (SIRET, IBAN, coordonnées des dirigeants) sont stockées en clair dans la base de données de production. Des exports CSV non chiffrés contenant l'intégralité des données clients sont présents sur les postes de développeurs pour les tests de non-régression.

Impact : En cas de compromission d'un poste de développeur ou de la base de données, l'ensemble des données de 12 clients PME industrielles (raisons sociales, IBAN, CA, contacts dirigeants) serait exposé. Violation majeure du RGPD (Art. 32 et 33).

4.5 Sécurité de l'infrastructure de déploiement

Référence	CS-2026-0847-05	**Criticité**	**HAUTE**
CVSS 3.1	7.2	**CWE**	CWE-250 (Execution with Unnecessary Privileges)

Constat : Plusieurs binaires sur les serveurs internes disposent du bit SUID sans justification opérationnelle. Le pipeline CI/CD Azure DevOps utilise un token à privilèges élevés (Personal Access Token avec scope complet) stocké en variable d'environnement.

5. Matrice des risques

Ref.	Vulnérabilité	Criticité	Exploitabilité	Priorité
CS-01	Secrets en clair	CRITIQUE	Triviale	P1
CS-02	API sans authentification	CRITIQUE	Facile	P1
CS-03	Mots de passe faibles	HAUTE	Facile	P2
CS-04	Données clients en clair	CRITIQUE	Modérée	P1
CS-05	SUID + privilèges CI/CD	HAUTE	Modérée	P2

6. Recommandations prioritaires

Actions immédiates (sous 15 jours) :

1. Rotation de tous les secrets exposés : changer l'ensemble des mots de passe, clés API, tokens et secrets JWT présents dans les fichiers de configuration. Invalider les tokens Azure DevOps compromis.

2. Sécuriser les endpoints API critiques : ajouter une authentification OAuth2/OIDC sur /api/v2/clients/export et /api/v2/admin/config. Implémenter un contrôle d'accès RBAC.

3. Supprimer les exports CSV des postes développeurs : les données de production ne doivent jamais être présentées sur les environnements de développement. Utiliser des jeux de données anonymisées.

Actions à moyen terme (sous 3 mois) :

4. Déployer un gestionnaire de secrets (HashiCorp Vault ou Azure Key Vault) et configurer l'injection de secrets au runtime.

5. Renforcer la politique de mots de passe AD et déployer le MFA sur SSH et VPN.

6. Auditer les binaires SUID et supprimer les privilèges non justifiés.

7. Chiffrer les données clients sensibles en base (IBAN, coordonnées) via AES-256.

7. Prochaines étapes

Ce pré-rapport est transmis à la Direction Générale d'Iron4Software pour une première prise de connaissance des constats majeurs. Nous recommandons vivement que l'équipe technique (et en particulier le responsable du module ERP Indus Portal) prenne connaissance de ces constats dans les meilleurs délais afin d'initier les actions correctives.

Echeance	Action	Responsable
14 fev. 2026	Transmission du pré-rapport a la DG	CyberShield Consulting
21 fev. 2026	Réunion de restitution technique	CyberShield + Equipe Dev Iron4
28 fev. 2026	Livraison du rapport final	CyberShield Consulting
15 mars 2026	Point d'avancement sur les remédiations P1	Iron4Software
Avril 2026	Contre-audit de vérification	CyberShield Consulting

Marc Delacroix
Directeur d'audit - CyberShield Consulting
CISSP | CEH | Lead Auditor ISO 27001
m.delacroix@cybershield-consulting.fr

CONFIDENTIEL - Ce document est la propriété de CyberShield Consulting SARL et est destine exclusivement a Iron4Software SAS. Toute reproduction ou diffusion non autorisée est strictement interdite. CyberShield Consulting SARL - SIRET 892 456 789 00012 - 47 Rue de Monceau, 75008 Paris - www.cybershield-consulting.fr