

CABINET DÉMO

Audit conteneurs et dépendances

Rapport d'audit de sécurité

PRÉPARÉ PAR

Cabinet Démo

DATE

05/08/2026

PÉRIMÈTRE

Images applicatives

Tableau de bord exécutif

16 VULNÉRABILITÉS	4 CRITIQUES	7 ÉLEVÉES
2 ACTIFS CONCERNÉS	7.7 CVSS MOYEN	2 À DISTANCE / SANS AUTHENTIFICATION

90 /100 SCORE DE RISQUE	POSTURE GLOBALE Exposition critique Le score est un indice d'exposition pondéré (0 = maîtrisée, 100 = critique) calculé à partir de la sévérité, du CVSS et de l'exploitabilité. Il ne mesure aucune conformité. RÉPARTITION PAR SÉVÉRITÉ CRITIQUE 4 · ÉLEVÉE 7 · MOYENNE 5
-----------------------------------	--

Impact métier

Conséquences concrètes pour l'activité si les expositions majeures ne sont pas traitées.

F-001 CVE-2021-44228 in log4js 6.3.0 Une exploitation peut permettre l'exécution de code arbitraire sur le service exposant cette image, avec un risque de compromission complète de l'application. HOST-01
F-002 CVE-2021-3711 in openssl 1.1.1k Une exploitation peut entraîner une corruption mémoire ou une exécution de code sur les composants utilisant cette bibliothèque cryptographique. HOST-01
F-003 CVE-2022-3602 in openssl 3.0.5-1 Une exploitation peut compromettre l'intégrité des échanges chiffrés et permettre l'exécution de code sur les systèmes concernés. HOST-01

Chemin d'attaque

PRISE DE PIED	F-001 CVE-2021-44228 in log4js 6.3.0 HOST-01 Sans authentification
ÉLEVATION	F-002 CVE-2021-3711 in openssl 1.1.1k HOST-01 Exécution de code
IMPACT MÉTIER	Fuite de données, interruption de service et exposition réglementaire.

Enchaînement le plus plausible entre l'accès externe et l'impact métier, à partir des constats ci-dessus. Les étapes non étayées par un constat ne sont pas représentées.

Feuille de route de remédiation

Phase 1 IMMÉDIAT · 0-7 JOURS 4 FINDINGS

Contenir l'exécution de code à distance et les accès non authentifiés.

Responsable: Infrastructure & DevOps · Charge: Moyenne
F-001, F-002, F-003, F-004

Phase 2 COURT TERME · 8-30 JOURS 7 FINDINGS

Corriger les services en sévérité élevée et supprimer les identifiants faibles.

Responsable: Infrastructure & DevOps · Charge: Moyenne
F-005, F-006, F-007, F-008, F-009, F-010 ...

Phase 3 MOYEN TERME · 31-90 JOURS 5 FINDINGS

Durcir la configuration, le TLS et la supervision ; retester le périmètre.

Responsable: Infrastructure & DevOps · Charge: Moyenne
F-012, F-013, F-014, F-015, F-016

Contrôle du document

VERSION	1.0
DATE	05/08/2026
AUTEUR	Cabinet Démo
CLASSIFICATION	Confidentiel — diffusion restreinte
DIFFUSION	Client et cabinet émetteur ; ne pas rediffuser sans accord écrit.
CONTACT	Non renseigné

Synthèse exécutive

L'audit a porté sur les images et composants logiciels utilisés par l'application, afin d'identifier les vulnérabilités présentes dans leurs briques techniques. Plusieurs failles critiques et importantes ont été identifiées, notamment sur des bibliothèques largement utilisées (chiffrement, compression, journalisation). Ces failles pourraient, si elles étaient exploitées, permettre une prise de contrôle partielle ou totale de certains services. Aucune preuve d'exploitation active n'a été constatée à ce stade. Une décision de priorisation des corrections est nécessaire, en particulier sur les composants critiques identifiés, afin de réduire l'exposition avant qu'une exploitation ne survienne.

Risques majeurs

- Une prise de contrôle d'un service applicatif est possible via des failles critiques touchant des bibliothèques de journalisation et de chiffrement, ce qui pourrait interrompre l'activité ou exposer des données.
- La compromission des échanges chiffrés est envisageable via plusieurs failles dans les bibliothèques cryptographiques, ce qui menacerait la confidentialité des communications avec les clients ou partenaires.
- Une élévation de privilèges ou une exécution de commandes non autorisées sur les systèmes hébergeant l'application pourrait permettre à un attaquant d'étendre son accès au-delà du périmètre initial.

Répartition par sévérité

SÉVÉRITÉ	#	%	
CRITIQUE	4	25%	
ÉLEVÉE	7	44%	
MOYENNE	5	31%	
FAIBLE	0	0%	
INFO	0	0%	

Périmètre et méthodologie

Dans le périmètre

Images applicatives

2 host(s)

HOST-01, HOST-02

Hors périmètre

Tout actif non présent dans les exports fournis. Aucune exploitation active, aucun test d'ingénierie sociale, aucun test de déni de service.

Fichiers analysés

FICHIER	OUTIL DÉTECTÉ	ÉTAT
trivy-api-image.json	TRIVY	Analysé
trivy-worker-image.json	TRIVY	Analysé

Méthodologie et limites

Les données proviennent d'exports de scanners automatisés (Nmap, Nessus, Trivy, Nuclei). Les findings sont corrélés et dédoublés entre outils, scorés à partir du CVSS et rattachés aux contrôles techniques pertinents.

Aucun enrichissement externe n'a pu être appliqué (CISA KEV et EPSS indisponibles) : la notation repose uniquement sur le CVSS et les sévérités rapportées par les outils.

Ce rapport est établi à partir de scans automatisés et ne constitue pas un test d'intrusion complet.

This report is based on automated scans and does not constitute a full penetration test.

Méthode de notation et de priorisation

Échelle de sévérité

SÉVÉRITÉ	CVSS
CRITIQUE / CRITICAL	9.0 - 10.0
ÉLEVÉE / HIGH	7.0 - 8.9
MOYENNE / MEDIUM	4.0 - 6.9
FAIBLE / LOW	0.1 - 3.9
INFO	0.0

Ajustements appliqués

Deux ajustements peuvent relever la sévérité d'un niveau, plafonnés à CRITIQUE. Chaque ajustement appliqué est indiqué sur la fiche du finding concerné :

- +1 niveau — exposition publique constatée (port ouvert sur une adresse routable).
- +1 niveau — exploitation connue (présence au catalogue CISA KEV, ou exploit signalé par l'outil de scan).

Aucun pourcentage de conformité n'est calculé. Les contrôles cités sont des éléments de preuve, la décision de conformité appartient à l'auditeur.

Signification des priorités

PRIORITÉ	
1	À traiter immédiatement / Immediate
2	À planifier dans le cycle courant / Planned
3	À suivre / Monitor

Synthèse des findings

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	PRIORITÉ	STATUT
F-001	CVE-2021-44228 in log4js 6.3.0	CRITIQUE	10.0	1	Ouvert
F-002	CVE-2021-3711 in openssl 1.1.1k	CRITIQUE	9.8	1	Ouvert
F-003	CVE-2022-3602 in openssl 3.0.5-1	CRITIQUE	9.8	1	Ouvert
F-004	CVE-2022-37434 in zlib 1.2.12-r1	CRITIQUE	9.8	1	Ouvert
F-005	CVE-2022-28391 in busybox 1.35.0-r17	ÉLEVÉE	8.8	2	Ouvert
F-006	CVE-2023-38545 in curl 7.83.1-r3	ÉLEVÉE	8.8	2	Ouvert
F-007	CVE-2023-4911 in glibc 2.31-13	ÉLEVÉE	7.8	2	Ouvert
F-008	CVE-2022-3786 in openssl 3.0.5-1	ÉLEVÉE	7.5	2	Ouvert
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	ÉLEVÉE	7.5	2	Ouvert
F-010	CVE-2020-8203 in lodash 4.17.15	ÉLEVÉE	7.4	2	Ouvert
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	ÉLEVÉE	7.4	2	Ouvert
F-012	CVE-2022-42898 in krb5 1.18.3-6	MOYENNE	6.5	3	Ouvert
F-013	CVE-2023-32681 in requests 2.28.1	MOYENNE	6.1	3	Ouvert
F-014	CVE-2023-29491 in ncurses 6.2-1	MOYENNE	5.5	3	Ouvert
F-015	CVE-2024-22195 in jinja2 3.0.3	MOYENNE	5.4	3	Ouvert
F-016	CVE-2022-25883 in semver 7.3.5	MOYENNE	5.3	3	Ouvert

Findings — détail

Extrait : 3 findings sur 16 sont détaillés ci-dessous. Les 13 findings restants, leurs preuves et leur plan de remédiation figurent dans le rapport complet.

F-001 CVE-2021-44228 in log4js 6.3.0

CRITIQUE CVSS 10.0 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H CWE-502 CVE-2021-44228 Sources: TRIVY

Sévérité critical : score CVSS de 10.0.

Détail CVSS — Vecteur d'attaque: Réseau · Complexité: Faible · Privilèges requis: Aucun · Interaction utilisateur: Aucune · Portée: Modifiée · Confidentialité: Élevé · Intégrité: Élevé · Disponibilité: Élevé

ACTIFS CONCERNÉS

HOST-01

L'image HOST-03/api:1.4.2 embarque la bibliothèque log4js en version 6.3.0, affectée par la vulnérabilité CVE-2021-44228. Un correctif est disponible en version 6.4.0. Cette faille permet une désérialisation non sécurisée.

IMPACT

Une exploitation peut permettre l'exécution de code arbitraire sur le service exposant cette image, avec un risque de compromission complète de l'application.

PREUVE

```
Target: app/package-lock.json
Package: log4js
Installed version: 6.3.0
Fixed version: 6.4.0
Vulnerability: CVE-2021-44228
```

VÉRIFICATION

Pour vérifier, exécuter : `trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour log4js vers la version 6.4.0 ou supérieure. Reconstruire et republier l'image applicative. Vérifier l'absence de dépendances transitives vulnérables. Réanalyser l'image après correction.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

<https://cwe.mitre.org/data/definitions/502.html>

Contrôles rattachés: A.8.8, 21.2.e · Statut: Ouvert

F-002 CVE-2021-3711 in openssl 1.1.1k

CRITIQUE CVSS 9.8 CWE-787 CVE-2021-3711 Sources: TRIVY

Sévérité critical : score CVSS de 9.8.

ACTIFS CONCERNÉS

HOST-01

L'image HOST-03/api:1.4.2 utilise openssl en version 1.1.1k, vulnérable à CVE-2021-3711. Le correctif est disponible en version 1.1.1l. Cette faille relève d'un dépassement de tampon.

IMPACT

Une exploitation peut entraîner une corruption mémoire ou une exécution de code sur les composants utilisant cette bibliothèque cryptographique.

PREUVE

```
Target: HOST-03/api:1.4.2 (debian 11.6)
Package: openssl
Installed version: 1.1.1k
Fixed version: 1.1.1l
Vulnerability: CVE-2021-3711
```

VÉRIFICATION

Pour vérifier, exécuter : `trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour le paquet openssl vers la version 1.1.1l. Reconstruire l'image à partir d'une base à jour. Réanalyser l'image après mise à jour.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2021-3711>

<https://cwe.mitre.org/data/definitions/787.html>

Contrôles rattachés: A.8.8, 21.2.e · Statut: Ouvert

F-003 CVE-2022-3602 in openssl 3.0.5-1

CRITIQUE CVSS 9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-787 CVE-2022-3602 Sources: TRIVY

Sévérité critical : score CVSS de 9.8.

Détail CVSS — Vecteur d'attaque: Réseau · Complexité: Faible · Privilèges requis: Aucun · Interaction utilisateur: Aucune · Portée: Inchangée · Confidentialité: Élevé · Intégrité: Élevé · Disponibilité: Élevé

ACTIFS CONCERNÉS

HOST-01

L'image HOST-03/api:1.4.2 embarque openssl en version 3.0.5-1, affectée par CVE-2022-3602. Le correctif est disponible en version 3.0.7-1. La vulnérabilité concerne un dépassement de tampon.

IMPACT

Une exploitation peut compromettre l'intégrité des échanges chiffrés et permettre l'exécution de code sur les systèmes concernés.

PREUVE

```
Target: HOST-03/api:1.4.2 (debian 11.6)
Package: openssl
Installed version: 3.0.5-1
Fixed version: 3.0.7-1
Vulnerability: CVE-2022-3602
```

VÉRIFICATION

Pour vérifier, exécuter : `trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour openssl vers la version 3.0.7-1 ou ultérieure. Reconstruire et republier l'image. Réanalyser l'image après correction.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2022-3602>

<https://cwe.mitre.org/data/definitions/787.html>

Contrôles rattachés: A.8.8, 21.2.e · Statut: Ouvert

Plan de remédiation

Immédiat (priorité 1)

Ce plan de remédiation s'organise en trois niveaux de priorité selon la criticité des vulnérabilités identifiées. Les quatre vulnérabilités critiques doivent être traitées sans délai : F-001 (log4js 6.3.0), F-002 (openssl 1.1.1k), F-003 (openssl 3.0.5-1) et F-004 (zlib 1.2.12-r1). Aucune de ces vulnérabilités n'est référencée au catalogue KEV, mais leur niveau de sévérité critique justifie une correction prioritaire, via mise à jour des composants concernés. Il convient de vérifier la disponibilité de correctifs pour chaque composant avant déploiement.

F-001 — CVE-2021-44228 in log4js 6.3.0

F-002 — CVE-2021-3711 in openssl 1.1.1k

F-003 — CVE-2022-3602 in openssl 3.0.5-1

F-004 — CVE-2022-37434 in zlib 1.2.12-r1

À planifier (priorité 2)

Sept vulnérabilités de sévérité élevée sont à intégrer au cycle de correction courant : F-005 (busybox), F-006 (curl), F-007 (glibc), F-008 et F-009 (openssl), F-010 (lodash) et F-011 (openssl). Ces éléments ne sont pas classés critiques ni référencés KEV, mais leur sévérité élevée justifie une planification dans le cycle de patch en cours. La mise à jour des versions concernées permettra de traiter l'ensemble de ce lot.

F-005 — CVE-2022-28391 in busybox 1.35.0-r17

F-006 — CVE-2023-38545 in curl 7.83.1-r3

F-007 — CVE-2023-4911 in glibc 2.31-13

F-008 — CVE-2022-3786 in openssl 3.0.5-1

F-009 — CVE-2022-4450 in openssl 1.1.1q-r0

F-010 — CVE-2020-8203 in lodash 4.17.15

F-011 — CVE-2023-0286 in openssl 1.1.1q-r0

À surveiller (priorité 3)

Cinq vulnérabilités de sévérité moyenne sont à surveiller sans action immédiate : F-012 (krb5), F-013 (requests), F-014 (ncurses), F-015 (jinja2) et F-016 (semver). Ces findings ne présentent pas de statut KEV et leur sévérité modérée ne requiert pas de traitement urgent. Un suivi périodique de ces composants est recommandé pour anticiper une éventuelle évolution de leur criticité.

F-012 — CVE-2022-42898 in krb5 1.18.3-6

F-013 — CVE-2023-32681 in requests 2.28.1

F-014 — CVE-2023-29491 in ncurses 6.2-1

F-015 — CVE-2024-22195 in jinja2 3.0.3

F-016 — CVE-2022-25883 in semver 7.3.5

Annexe — Rattachement aux contrôles

Ces éléments constituent des preuves techniques rattachées aux contrôles ci-dessous. Ils ne constituent pas une évaluation de conformité : aucun pourcentage n'est calculé, la décision de conformité appartient à l'auditeur.

CONTRÔLE	INTITULÉ	FINDINGS
A.8.8	Management of technical vulnerabilities	F-001, F-002, F-003, F-004, F-005, F-006, F-007, F-008, F-009, F-010, F-011, F-012, F-013, F-014, F-015, F-016

NIS2

MESURE	INTITULÉ	FINDINGS
21.2.e	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	F-001, F-002, F-003, F-004, F-005, F-006, F-007, F-008, F-009, F-010, F-011, F-012, F-013, F-014, F-015, F-016

Annexe technique

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	ACTIFS
F-001	CVE-2021-44228 in log4js 6.3.0	CRITIQUE	10.0	1
F-002	CVE-2021-3711 in openssl 1.1.1k	CRITIQUE	9.8	1
F-003	CVE-2022-3602 in openssl 3.0.5-1	CRITIQUE	9.8	1
F-004	CVE-2022-37434 in zlib 1.2.12-r1	CRITIQUE	9.8	1
F-005	CVE-2022-28391 in busybox 1.35.0-r17	ÉLEVÉE	8.8	1
F-006	CVE-2023-38545 in curl 7.83.1-r3	ÉLEVÉE	8.8	2
F-007	CVE-2023-4911 in glibc 2.31-13	ÉLEVÉE	7.8	1
F-008	CVE-2022-3786 in openssl 3.0.5-1	ÉLEVÉE	7.5	1
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	ÉLEVÉE	7.5	1
F-010	CVE-2020-8203 in lodash 4.17.15	ÉLEVÉE	7.4	1
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	ÉLEVÉE	7.4	1
F-012	CVE-2022-42898 in krb5 1.18.3-6	MOYENNE	6.5	1
F-013	CVE-2023-32681 in requests 2.28.1	MOYENNE	6.1	1
F-014	CVE-2023-29491 in ncurses 6.2-1	MOYENNE	5.5	1
F-015	CVE-2024-22195 in jinja2 3.0.3	MOYENNE	5.4	1
F-016	CVE-2022-25883 in semver 7.3.5	MOYENNE	5.3	1

Annexe — Re-test

À compléter lors du contrôle de remédiation.

RÉF	INTITULÉ	STATUT	DATE	VÉRIFICATION
F-001	CVE-2021-44228 in log4js 6.3.0	Ouvert		
F-002	CVE-2021-3711 in openssl 1.1.1k	Ouvert		
F-003	CVE-2022-3602 in openssl 3.0.5-1	Ouvert		
F-004	CVE-2022-37434 in zlib 1.2.12-r1	Ouvert		
F-005	CVE-2022-28391 in busybox 1.35.0-r17	Ouvert		
F-006	CVE-2023-38545 in curl 7.83.1-r3	Ouvert		
F-007	CVE-2023-4911 in glibc 2.31-13	Ouvert		
F-008	CVE-2022-3786 in openssl 3.0.5-1	Ouvert		
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	Ouvert		
F-010	CVE-2020-8203 in lodash 4.17.15	Ouvert		
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	Ouvert		
F-012	CVE-2022-42898 in krb5 1.18.3-6	Ouvert		
F-013	CVE-2023-32681 in requests 2.28.1	Ouvert		
F-014	CVE-2023-29491 in ncurses 6.2-1	Ouvert		
F-015	CVE-2024-22195 in jinja2 3.0.3	Ouvert		
F-016	CVE-2022-25883 in semver 7.3.5	Ouvert		