

CABINET DÉMO

Preuves techniques ISO 27001 / NIS2

Rapport d'audit de sécurité

PRÉPARÉ PAR Cabinet Démo

DATE 05/08/2026

PÉRIMÈTRE Périmètre audité

Tableau de bord exécutif

40 VULNÉRABILITÉS	13 CRITIQUES	15 ÉLEVÉES
9 ACTIFS CONCERNÉS	8.0 CVSS MOYEN	9 À DISTANCE / SANS AUTHENTIFICATION

100 /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 13 · ÉLEVÉE 15 · MOYENNE 9 · FAIBLE 3
------------------------------------	---

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 de cette vulnérabilité peut permettre l'exécution de code à distance sur le composant applicatif concerné, compromettant la disponibilité et l'intégrité du service. HOST-01
F-002 vsftpd Smiley Face Backdoor Une exploitation de cette porte dérobée peut permettre un accès non autorisé au serveur avec un contrôle étendu, exposant les données hébergées et les systèmes adjacents. NET-A-H1:21
F-003 Apache 2.4.x < 2.4.51 Path Traversal Une exploitation de cette vulnérabilité peut permettre la lecture de fichiers sensibles ou l'exécution de code sur le serveur, compromettant la confidentialité et l'intégrité des données hébergées. NET-B-H1:80

Chemin d'attaque

PRISE DE PIED	F-001 CVE-2021-44228 in log4js 6.3.0 HOST-01 Sans authentification
ÉLEVATION	F-003 Apache 2.4.x < 2.4.51 Path Traversal NET-B-H1:80 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 15 FINDINGS

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

Responsable: Ingénierie sécurité · Charge: Élevée
F-001, F-002, F-003, F-004, F-005, F-006 ...

Phase 2 COURT TERME · 8-30 JOURS 13 FINDINGS

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

Responsable: Infrastructure & DevOps · Charge: Élevée
F-014, F-015, F-016, F-019, F-020, F-021 ...

Phase 3 MOYEN TERME · 31-90 JOURS 12 FINDINGS

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

Responsable: Infrastructure & DevOps · Charge: Élevée
F-029, F-030, F-031, F-032, F-033, F-034 ...

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 un ensemble de composants applicatifs et de bases de données exposés. Il ressort un nombre élevé de vulnérabilités critiques, notamment des accès non authentifiés à plusieurs bases de données et interfaces d'administration, ainsi que des failles connues sur des composants logiciels tiers. Ces faiblesses, prises ensemble, permettraient à un attaquant d'accéder aux données de l'entreprise ou de perturber les services concernés. Une décision doit être prise rapidement sur la priorisation et le financement des actions correctives, en particulier sur les accès aux bases de données et aux outils d'administration. Sans action, l'exposition actuelle constitue un risque direct pour la continuité d'activité et la confidentialité des données.

Risques majeurs

- Des bases de données et outils d'administration accessibles sans authentification pourraient permettre à un tiers de consulter, modifier ou détruire des données métier sensibles.
- Plusieurs failles critiques sur des composants applicatifs pourraient permettre à un attaquant de prendre le contrôle de serveurs, entraînant une interruption de service.
- Une vulnérabilité sur l'équipement réseau Fortinet pourrait exposer des identifiants d'accès et compromettre l'ensemble du réseau interne de l'entreprise.

Répartition par sévérité

SÉVÉRITÉ	#	%	
CRITIQUE	13	32%	
ÉLEVÉE	15	38%	
MOYENNE	9	22%	
FAIBLE	3	8%	
INFO	0	0%	

Périmètre et méthodologie

Dans le périmètre

Périmètre audité

9 host(s)

HOST-01, NET-A-H1, NET-B-H1, HOST-04, NET-B-H2, NET-C-H1, NET-C-H2, NET-B-H3, NET-B-H4

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
nmap-engagement.xml	NMAP	Analysé
nessus-engagement.nessus	NESSUS	Analysé
nuclei-engagement.jsonl	NUCLEI	Analysé
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 dédupliqués 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	vsftpd Smiley Face Backdoor	CRITIQUE	10.0	1	Ouvert
F-003	Apache 2.4.x < 2.4.51 Path Traversal	CRITIQUE	9.8	1	Ouvert
F-004	CVE-2021-3711 in openssl 1.1.1k	CRITIQUE	9.8	1	Ouvert
F-005	CVE-2022-3602 in openssl 3.0.5-1	CRITIQUE	9.8	1	Ouvert
F-006	CVE-2022-37434 in zlib 1.2.12-r1	CRITIQUE	9.8	1	Ouvert
F-007	Fortinet FortiOS Path Traversal	CRITIQUE	9.8	1	Ouvert
F-008	Jenkins unauthenticated dashboard	CRITIQUE	9.8	1	Ouvert
F-009	MongoDB Unauthenticated Access	CRITIQUE	9.8	1	Ouvert
F-010	MySQL Unpassworded Account Check	CRITIQUE	9.8	1	Ouvert
F-011	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITIQUE	9.8	1	Ouvert
F-012	PostgreSQL Default Credentials	CRITIQUE	9.8	1	Ouvert
F-013	Redis Server Unprotected Access	CRITIQUE	9.8	1	Ouvert
F-014	CVE-2022-28391 in busybox 1.35.0-r17	ÉLEVÉE	8.8	2	Ouvert
F-015	CVE-2023-38545 in curl 7.83.1-r3	ÉLEVÉE	8.8	2	Ouvert
F-016	Jenkins < 2.235.2 Multiple Vulnerabilities	ÉLEVÉE	8.8	2	Ouvert
F-017	Tomcat manager default credentials	ÉLEVÉE	8.8	1	Ouvert
F-018	MS17-010 SMB Remote Code Execution	ÉLEVÉE	8.1	1	Ouvert
F-019	CVE-2023-4911 in glibc 2.31-13	ÉLEVÉE	7.8	2	Ouvert
F-020	CVE-2022-3786 in openssl 3.0.5-1	ÉLEVÉE	7.5	2	Ouvert
F-021	CVE-2022-4450 in openssl 1.1.1q-r0	ÉLEVÉE	7.5	2	Ouvert
F-022	Elasticsearch Unauthenticated Access	ÉLEVÉE	7.5	2	Ouvert
F-023	Exposed .env file	ÉLEVÉE	7.5	2	Ouvert
F-024	SMTP Service STARTTLS Plaintext	ÉLEVÉE	7.5	2	Ouvert

Injection					
F-025	SSL Certificate Cannot Be Trusted	ÉLEVÉE	7.5	2	Ouvert
F-026	Unencrypted Telnet Server	ÉLEVÉE	7.5	2	Ouvert
F-027	CVE-2020-8203 in lodash 4.17.15	ÉLEVÉE	7.4	2	Ouvert
F-028	CVE-2023-0286 in openssl 1.1.1q-r0	ÉLEVÉE	7.4	2	Ouvert
F-029	CVE-2022-42898 in krb5 1.18.3-6	MOYENNE	6.5	3	Ouvert
F-030	CVE-2023-32681 in requests 2.28.1	MOYENNE	6.1	3	Ouvert
F-031	CVE-2023-29491 in ncurses 6.2-1	MOYENNE	5.5	3	Ouvert
F-032	CVE-2024-22195 in jinja2 3.0.3	MOYENNE	5.4	3	Ouvert
F-033	CVE-2022-25883 in semver 7.3.5	MOYENNE	5.3	3	Ouvert
F-034	OpenSSH < 7.9 User Enumeration	MOYENNE	5.3	3	Ouvert
F-035	SSH Weak Algorithms Supported	MOYENNE	5.3	3	Ouvert
F-036	SSL Medium Strength Cipher Suites Supported	MOYENNE	5.3	3	Ouvert
F-037	Terminal Services Doesn't Use NLA	MOYENNE	5.3	3	Ouvert
F-038	Observations de sévérité faible — exposition d'informations	FAIBLE		3	Ouvert
F-039	Observations de sévérité faible — chiffrement TLS	FAIBLE		3	Ouvert
F-040	Observations de sévérité faible — services web	FAIBLE		3	Ouvert

Findings — détail

Extrait : 3 findings sur 40 sont détaillés ci-dessous. Les 37 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

La bibliothèque log4js en version 6.3.0 est utilisée dans l'image HOST-10/api:1.4.2. Cette version est affectée par la vulnérabilité CVE-2021-44228, corrigée en version 6.4.0. La faille a été détectée par analyse de composants (Trivy) sur le fichier package-lock.json.

IMPACT

Une exploitation de cette vulnérabilité peut permettre l'exécution de code à distance sur le composant applicatif concerné, compromettant la disponibilité et l'intégrité du service.

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 la commande : `trivy image --severity HIGH,CRITICAL HOST-10/api:1.4.2`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour le paquet log4js vers la version 6.4.0 ou supérieure. Reconstruire et republier l'image applicative. Revalider l'absence de la vulnérabilité par un nouveau scan de composants. Intégrer ce contrôle dans le pipeline CI/CD pour éviter la régression.

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 vsftpd Smiley Face Backdoor

CRITIQUE CVSS 10.0 CVE-2011-2523 Sources: NESSUS, NMAP

Sévérité critical : score CVSS de 10.0.

ACTIFS CONCERNÉS

NET-A-H1:21

Le service FTP exposé sur NET-A-H1:21 exécute vsftpd en version 2.3.4. Cette version correspond à une porte dérobée connue (Smiley Face Backdoor), identifiée par les sources Nessus et Nmap.

IMPACT

Une exploitation de cette porte dérobée peut permettre un accès non autorisé au serveur avec un contrôle étendu, exposant les données hébergées et les systèmes adjacents.

PREUVE

```
<port protocol="tcp" portid="21">
  <state state="open" reason="syn-ack"/>
  <service name="ftp" product="vsftpd" version="2.3.4" method="probed" conf="10"/>
</port>
```

VÉRIFICATION

Pour vérifier, rejouer le plugin Nessus 52703 sur NET-A-H1, puis exécuter la commande : `nmap -p21 -sV --script vulners NET-A-H1`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre hors service ou remplacer immédiatement ce service vsftpd. Déployer une version maintenue et à jour du serveur FTP. Restreindre l'exposition du service FTP au strict nécessaire via des règles de filtrage réseau. Auditer les journaux d'accès pour détecter une éventuelle compromission antérieure.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2011-2523>

<https://www.tenable.com/plugins/nessus/52703>

Contrôles rattachés: A.8.8, A.8.12, A.8.3, A.8.21, A.8.5, 21.2.e, 21.2.i · Statut: Ouvert

F-003 Apache 2.4.x < 2.4.51 Path Traversal

CRITIQUE CVSS 9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-22 CVE-2021-41773, CVE-2021-42013
Sources: NESSUS, NMAP, NUCLEI

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

NET-B-H1:80

Le serveur web exposé sur NET-B-H1:80 exécute Apache en version 2.4.29, inférieure à la version corrigée 2.4.51. Cette version est vulnérable à une traversée de chemin permettant potentiellement une exécution de code, identifiée par plusieurs sources (Nessus, Nmap, Nuclei).

IMPACT

Une exploitation de cette vulnérabilité peut permettre la lecture de fichiers sensibles ou l'exécution de code sur le serveur, compromettant la confidentialité et l'intégrité des données hébergées.

PREUVE

Installed version : 2.4.29

```
<port protocol="tcp" portid="80">
  <state state="open" reason="syn-ack"/>
  <service name="http" product="Apache httpd" version="2.4.29" method="probed" conf="10"/>
  <script id="vulners" output="&#10; cpe:/a:apache:http_server:2.4.29:&#10; CVE-2021-41773 9.8
https://vulners.com/cve/CVE-2021-41773&#10; CVE-2021-42013 9.8 https://vulners.com/cve/CVE-2021-
42013&#10;"/>
</port>
```

Template: CVE-2021-41773

Matched at: `http://NET-B-H1/cgi-bin/.%2e/%2e/%2e/etc/passwd`

Extracted: `root:x:0:0:root:/root:/bin/bash`

VÉRIFICATION

Pour vérifier, rejouer le plugin Nessus 156032 sur NET-B-H1, exécuter la commande `nmap -p80 -sV --script vulners NET-B-H1`, puis `nuclei -id CVE-2021-41773 -u http://NET-B-H1`

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour Apache vers une version corrigée (2.4.51 ou ultérieure). Vérifier la configuration des répertoires et désactiver les modules non nécessaires. Revalider l'absence de la vulnérabilité après mise à jour via un nouveau scan.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2021-41773>

<https://nvd.nist.gov/vuln/detail/CVE-2021-42013>

<https://cwe.mitre.org/data/definitions/22.html>

<https://www.tenable.com/plugins/nessus/156032>

<https://github.com/projectdiscovery/nuclei-templates/search?q=CVE-2021-41773>

Contrôles rattachés: A.8.8, A.8.26, A.8.28, 21.2.e · Statut: Ouvert

Plan de remédiation

Immédiat (priorité 1)

Le plan de remédiation ci-dessous distingue trois niveaux de priorité en fonction de la sévérité et de la nature des findings identifiés. Les 15 findings de priorité 1 doivent être traités sans attendre, dont 13 de sévérité critique (F-001 à F-013) et 2 de sévérité haute (F-017, F-018). Ce lot regroupe des vulnérabilités logicielles critiques (log4js, openssl, zlib, Apache, Fortinet), des accès non authentifiés sur des services exposés (MongoDB, Redis, Jenkins, MySQL, PostgreSQL) et une porte dérobée connue sur vsftpd. La combinaison de sévérité critique et d'exposition directe de services justifie un traitement prioritaire, indépendamment de l'absence de statut KEV.

F-001 — CVE-2021-44228 in log4js 6.3.0
F-002 — vsftpd Smiley Face Backdoor
F-003 — Apache 2.4.x < 2.4.51 Path Traversal
F-004 — CVE-2021-3711 in openssl 1.1.1k
F-005 — CVE-2022-3602 in openssl 3.0.5-1
F-006 — CVE-2022-37434 in zlib 1.2.12-r1
F-007 — Fortinet FortiOS Path Traversal
F-008 — Jenkins unauthenticated dashboard
F-009 — MongoDB Unauthenticated Access
F-010 — MySQL Unpassworded Account Check
F-011 — OpenSSL 3.0.0 < 3.0.7 Buffer Overflow
F-012 — PostgreSQL Default Credentials
F-013 — Redis Server Unprotected Access
F-017 — Tomcat manager default credentials
F-018 — MS17-010 SMB Remote Code Execution

À planifier (priorité 2)

Les 13 findings de priorité 2, tous de sévérité haute, doivent être planifiés dans le cycle courant. Ce lot comprend des vulnérabilités applicatives (busybox, curl, glibc, openssl, lodash) ainsi que des expositions de configuration (fichier .env exposé, Telnet non chiffré, certificat SSL non fiable, STARTTLS en clair). Un traitement dans les prochaines itérations de maintenance est recommandé, sans urgence immédiate au regard des éléments fournis.

F-014 — CVE-2022-28391 in busybox 1.35.0-r17
F-015 — CVE-2023-38545 in curl 7.83.1-r3
F-016 — Jenkins < 2.235.2 Multiple Vulnerabilities
F-019 — CVE-2023-4911 in glibc 2.31-13
F-020 — CVE-2022-3786 in openssl 3.0.5-1
F-021 — CVE-2022-4450 in openssl 1.1.1q-r0
F-022 — Elasticsearch Unauthenticated Access
F-023 — Exposed .env file
F-024 — SMTP Service STARTTLS Plaintext Injection
F-025 — SSL Certificate Cannot Be Trusted
F-026 — Unencrypted Telnet Server
F-027 — CVE-2020-8203 in lodash 4.17.15
F-028 — CVE-2023-0286 in openssl 1.1.1q-r0

À surveiller (priorité 3)

Les 12 findings de priorité 3 sont à surveiller sans action immédiate, répartis entre 9 vulnérabilités de sévérité moyenne (krb5, requests, ncurses, jinja2, semver, OpenSSH, algorithmes SSH faibles, chiffrements SSL moyens, absence de NLA sur RDP) et 3 observations de sévérité basse relatives à l'exposition, au TLS et au web. Ces éléments ne présentent pas de caractère critique dans les données fournies mais méritent un suivi lors des cycles d'audit suivants.

- F-029 — CVE-2022-42898 in krb5 1.18.3-6
- F-030 — CVE-2023-32681 in requests 2.28.1
- F-031 — CVE-2023-29491 in ncurses 6.2-1
- F-032 — CVE-2024-22195 in jinja2 3.0.3
- F-033 — CVE-2022-25883 in semver 7.3.5
- F-034 — OpenSSH < 7.9 User Enumeration
- F-035 — SSH Weak Algorithms Supported
- F-036 — SSL Medium Strength Cipher Suites Supported
- F-037 — Terminal Services Doesn't Use NLA
- F-038 — Observations de sévérité faible — exposition d'informations
- F-039 — Observations de sévérité faible — chiffrement TLS
- F-040 — Observations de sévérité faible — services web

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.8.12	Data leakage prevention	F-002, F-009, F-013, F-023, F-038
A.8.20	Networks security	F-018, F-034, F-035
A.8.21	Security of network services	F-002, F-026, F-037
A.8.22	Segregation of networks	F-010, F-012, F-018, F-034, F-035
A.8.24	Use of cryptography	F-007, F-011, F-023, F-024, F-025, F-036, F-039
A.8.26	Application security requirements	F-003, F-007, F-008, F-018, F-022, F-024, F-040
A.8.28	Secure coding	F-003, F-007, F-008, F-018, F-022, F-024, F-040
A.8.3	Information access restriction	F-002, F-009, F-010, F-012, F-013, F-023, F-038
A.8.5	Secure authentication	F-002, F-012, F-017, F-026, F-037
A.8.8	Management of technical vulnerabilities	F-001, F-002, F-003, F-004, F-005, F-006, F-007, F-011, F-014, F-015, F-016, F-018, F-019, F-020, F-021, F-024, F-027, F-028, F-029, F-030, F-031, F-032, F-033, F-034
A.8.9	Configuration management	F-017

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-011, F-013, F-014, F-015, F-016, F-018, F-019, F-020, F-021, F-022, F-024, F-027, F-028, F-029, F-030, F-031, F-032, F-033, F-034, F-038, F-040
21.2.f	Policies to assess the effectiveness of cybersecurity risk-management measures	F-017

21.2.g	Basic cyber hygiene practices and cybersecurity training	F-017
21.2.h	Policies on the use of cryptography and, where appropriate, encryption	F-007, F-011, F-023, F-024, F-025, F-036, F-039
21.2.i	Human resources security, access control policies and asset management	F-002, F-009, F-010, F-012, F-013, F-017, F-034, F-035, F-038
21.2.j	Use of multi-factor authentication, secured communications and secured emergency communication systems	F-007, F-011, F-012, F-017, F-023, F-024, F-025, F-034, F-035, F-036, F-039

Annexe technique

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	ACTIFS
F-001	CVE-2021-44228 in log4js 6.3.0	CRITIQUE	10.0	1
F-002	vsftpd Smiley Face Backdoor	CRITIQUE	10.0	1
F-003	Apache 2.4.x < 2.4.51 Path Traversal	CRITIQUE	9.8	1
F-004	CVE-2021-3711 in openssl 1.1.1k	CRITIQUE	9.8	1
F-005	CVE-2022-3602 in openssl 3.0.5-1	CRITIQUE	9.8	1
F-006	CVE-2022-37434 in zlib 1.2.12-r1	CRITIQUE	9.8	1
F-007	Fortinet FortiOS Path Traversal	CRITIQUE	9.8	1
F-008	Jenkins unauthenticated dashboard	CRITIQUE	9.8	1
F-009	MongoDB Unauthenticated Access	CRITIQUE	9.8	1
F-010	MySQL Unpassworded Account Check	CRITIQUE	9.8	1
F-011	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITIQUE	9.8	1
F-012	PostgreSQL Default Credentials	CRITIQUE	9.8	1
F-013	Redis Server Unprotected Access	CRITIQUE	9.8	1
F-014	CVE-2022-28391 in busybox 1.35.0-r17	ÉLEVÉE	8.8	1
F-015	CVE-2023-38545 in curl 7.83.1-r3	ÉLEVÉE	8.8	2
F-016	Jenkins < 2.235.2 Multiple Vulnerabilities	ÉLEVÉE	8.8	1
F-017	Tomcat manager default credentials	ÉLEVÉE	8.8	1
F-018	MS17-010 SMB Remote Code Execution	ÉLEVÉE	8.1	1
F-019	CVE-2023-4911 in glibc 2.31-13	ÉLEVÉE	7.8	1
F-020	CVE-2022-3786 in openssl 3.0.5-1	ÉLEVÉE	7.5	1
F-021	CVE-2022-4450 in openssl 1.1.1q-r0	ÉLEVÉE	7.5	1
F-022	Elasticsearch Unauthenticated Access	ÉLEVÉE	7.5	1
F-023	Exposed .env file	ÉLEVÉE	7.5	2
F-024	SMTP Service STARTTLS Plaintext Injection	ÉLEVÉE	7.5	1
F-025	SSL Certificate Cannot Be Trusted	ÉLEVÉE	7.5	1
F-026	Unencrypted Telnet Server	ÉLEVÉE	7.5	1
F-027	CVE-2020-8203 in lodash 4.17.15	ÉLEVÉE	7.4	1
F-028	CVE-2023-0286 in openssl 1.1.1q-r0	ÉLEVÉE	7.4	1

F-029	CVE-2022-42898 in krb5 1.18.3-6	MOYENNE	6.5	1
F-030	CVE-2023-32681 in requests 2.28.1	MOYENNE	6.1	1
F-031	CVE-2023-29491 in ncurses 6.2-1	MOYENNE	5.5	1
F-032	CVE-2024-22195 in jinja2 3.0.3	MOYENNE	5.4	1
F-033	CVE-2022-25883 in semver 7.3.5	MOYENNE	5.3	1
F-034	OpenSSH < 7.9 User Enumeration	MOYENNE	5.3	1
F-035	SSH Weak Algorithms Supported	MOYENNE	5.3	1
F-036	SSL Medium Strength Cipher Suites Supported	MOYENNE	5.3	2
F-037	Terminal Services Doesn't Use NLA	MOYENNE	5.3	1
F-038	Observations de sévérité faible — exposition d'informations	FAIBLE		5
F-039	Observations de sévérité faible — chiffrement TLS	FAIBLE		5
F-040	Observations de sévérité faible — services web	FAIBLE		6

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	vsftpd Smiley Face Backdoor	Ouvert		
F-003	Apache 2.4.x < 2.4.51 Path Traversal	Ouvert		
F-004	CVE-2021-3711 in openssl 1.1.1k	Ouvert		
F-005	CVE-2022-3602 in openssl 3.0.5-1	Ouvert		
F-006	CVE-2022-37434 in zlib 1.2.12-r1	Ouvert		
F-007	Fortinet FortiOS Path Traversal	Ouvert		
F-008	Jenkins unauthenticated dashboard	Ouvert		
F-009	MongoDB Unauthenticated Access	Ouvert		
F-010	MySQL Unpassworded Account Check	Ouvert		
F-011	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	Ouvert		
F-012	PostgreSQL Default Credentials	Ouvert		
F-013	Redis Server Unprotected Access	Ouvert		
F-014	CVE-2022-28391 in busybox 1.35.0-r17	Ouvert		
F-015	CVE-2023-38545 in curl 7.83.1-r3	Ouvert		
F-016	Jenkins < 2.235.2 Multiple Vulnerabilities	Ouvert		
F-017	Tomcat manager default credentials	Ouvert		
F-018	MS17-010 SMB Remote Code Execution	Ouvert		
F-019	CVE-2023-4911 in glibc 2.31-13	Ouvert		
F-020	CVE-2022-3786 in openssl 3.0.5-1	Ouvert		
F-021	CVE-2022-4450 in openssl 1.1.1q-r0	Ouvert		
F-022	Elasticsearch Unauthenticated Access	Ouvert		
F-023	Exposed .env file	Ouvert		
F-024	SMTP Service STARTTLS Plaintext Injection	Ouvert		
F-025	SSL Certificate Cannot Be Trusted	Ouvert		

F-026	Unencrypted Telnet Server	Ouvert
F-027	CVE-2020-8203 in lodash 4.17.15	Ouvert
F-028	CVE-2023-0286 in openssl 1.1.1q-r0	Ouvert
F-029	CVE-2022-42898 in krb5 1.18.3-6	Ouvert
F-030	CVE-2023-32681 in requests 2.28.1	Ouvert
F-031	CVE-2023-29491 in ncurses 6.2-1	Ouvert
F-032	CVE-2024-22195 in jinja2 3.0.3	Ouvert
F-033	CVE-2022-25883 in semver 7.3.5	Ouvert
F-034	OpenSSH < 7.9 User Enumeration	Ouvert
F-035	SSH Weak Algorithms Supported	Ouvert
F-036	SSL Medium Strength Cipher Suites Supported	Ouvert
F-037	Terminal Services Doesn't Use NLA	Ouvert
F-038	Observations de sévérité faible — exposition d'informations	Ouvert
F-039	Observations de sévérité faible — chiffrement TLS	Ouvert
F-040	Observations de sévérité faible — services web	Ouvert