

CABINET DÉMO

Test réseau interne

Rapport d'audit de sécurité

PRÉPARÉ PAR	Cabinet Démo
DATE	05/08/2026
PÉRIMÈTRE	Segment interne

Tableau de bord exécutif

22 VULNÉRABILITÉS	8 CRITIQUES	7 ÉLEVÉES
7 ACTIFS CONCERNÉS	7.7 CVSS MOYEN	5 À DISTANCE / SANS AUTHENTIFICATION

98 /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 8 · ÉLEVÉE 7 · MOYENNE 4 · FAIBLE 2 · INFO 1
-----------------------------------	--

Impact métier

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

F-001 vsftpd Smiley Face Backdoor Un attaquant peut obtenir un accès complet au système exposé, avec un risque de compromission totale de la machine et des données qu'elle héberge. NET-A-H1:21
F-002 Apache 2.4.x < 2.4.51 Path Traversal Un attaquant peut accéder à des fichiers sensibles du serveur ou exécuter du code arbitraire, compromettant la confidentialité et l'intégrité des données hébergées. NET-B-H1:80
F-003 Fortinet FortiOS Path Traversal Un attaquant peut récupérer des informations d'authentification et accéder au VPN ou à l'infrastructure protégée par cet équipement. NET-B-H2:443

Chemin d'attaque

PRISE DE PIED	F-002 Apache 2.4.x < 2.4.51 Path Traversal NET-B-H1:80 Sans authentification
ÉLEVATION	F-003 Fortinet FortiOS Path Traversal NET-B-H2:443 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 11 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 4 FINDINGS

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

Responsable: Ingénierie sécurité · Charge: Moyenne
F-009, F-013, F-014, F-015

Phase 3 MOYEN TERME · 31-90 JOURS 7 FINDINGS

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

Responsable: Ingénierie sécurité · Charge: Moyenne
F-016, F-017, F-018, F-019, F-020, F-021 ...

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 systèmes et services exposés, incluant serveurs web, bases de données, outils d'intégration continue et équipements réseau. Il révèle un nombre important de failles critiques permettant un accès non autorisé à des données ou une prise de contrôle de systèmes sans nécessiter d'authentification. Plusieurs bases de données et services sont accessibles sans mot de passe ou avec des identifiants par défaut, ce qui constitue un point d'entrée immédiat pour un attaquant. Une décision rapide est nécessaire pour prioriser la mise en sécurité des services exposés et restreindre les accès non authentifiés avant toute autre action. Sans intervention, l'entreprise s'expose à un risque élevé de fuite ou de perte de données ainsi qu'à une compromission durable de son infrastructure.

Risques majeurs

- Plusieurs bases de données critiques sont accessibles sans authentification, exposant l'ensemble des données de l'entreprise à un vol ou une destruction.
- Des serveurs et équipements réseau présentent des failles permettant une prise de contrôle complète à distance, avec un risque de paralysie de l'activité.
- La chaîne de développement logiciel (serveur d'intégration continue) est exposée, ce qui pourrait permettre à un attaquant de compromettre les futures versions des applications de l'entreprise.

Répartition par sévérité

SÉVÉRITÉ	#	%	
CRITIQUE	8	36%	
ÉLEVÉE	7	32%	
MOYENNE	4	18%	
FAIBLE	2	9%	
INFO	1	5%	

Périmètre et méthodologie

Dans le périmètre

Segment interne

7 host(s)

NET-A-H1, NET-B-H1, NET-B-H2, NET-C-H1, NET-B-H3, NET-B-H4, NET-C-H2

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

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	vsftpd Smiley Face Backdoor	CRITIQUE	10.0	1	Ouvert
F-002	Apache 2.4.x < 2.4.51 Path Traversal	CRITIQUE	9.8	1	Ouvert
F-003	Fortinet FortiOS Path Traversal	CRITIQUE	9.8	1	Ouvert
F-004	MongoDB Unauthenticated Access	CRITIQUE	9.8	1	Ouvert
F-005	MySQL Unpassworded Account Check	CRITIQUE	9.8	1	Ouvert
F-006	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITIQUE	9.8	1	Ouvert
F-007	PostgreSQL Default Credentials	CRITIQUE	9.8	1	Ouvert
F-008	Redis Server Unprotected Access	CRITIQUE	9.8	1	Ouvert
F-009	Jenkins < 2.235.2 Multiple Vulnerabilities	ÉLEVÉE	8.8	2	Ouvert
F-010	MS17-010 SMB Remote Code Execution	ÉLEVÉE	8.1	1	Ouvert
F-011	Elasticsearch Unauthenticated Access	ÉLEVÉE	7.5	1	Ouvert
F-012	Jenkins Anonymous Access Enabled	ÉLEVÉE	7.5	1	Ouvert
F-013	SMTP Service STARTTLS Plaintext Injection	ÉLEVÉE	7.5	2	Ouvert
F-014	SSL Certificate Cannot Be Trusted	ÉLEVÉE	7.5	2	Ouvert
F-015	Unencrypted Telnet Server	ÉLEVÉE	7.5	2	Ouvert
F-016	OpenSSH < 7.9 User Enumeration	MOYENNE	5.3	3	Ouvert
F-017	SSH Weak Algorithms Supported	MOYENNE	5.3	3	Ouvert
F-018	SSL Medium Strength Cipher Suites Supported	MOYENNE	5.3	3	Ouvert
F-019	Terminal Services Doesn't Use NLA	MOYENNE	5.3	3	Ouvert
F-020	HTTP TRACE / TRACK Methods Allowed	FAIBLE	3.7	3	Ouvert
F-021	TLS Version 1.0 Protocol Detection	FAIBLE	3.7	3	Ouvert
F-022	Observations de sévérité faible — exposition d'informations	INFO		3	Ouvert

Findings — détail

Extrait : 3 findings sur 22 sont détaillés ci-dessous. Les 19 findings restants, leurs preuves et leur plan de remédiation figurent dans le rapport complet.

F-001 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 vsftpd 2.3.4 détecté sur NET-A-H1:21 correspond à une version contenant une porte dérobée connue (Smiley Face Backdoor). Cette version permet une exécution de commandes à distance sans authentification préalable.

IMPACT

Un attaquant peut obtenir un accès complet au système exposé, avec un risque de compromission totale de la machine et des données qu'elle héberge.

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

Rejouer le plugin Nessus 52703 sur NET-A-H1 ; nmap -p21 -sV --script vulners NET-A-H1.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour vsftpd vers une version corrigée non affectée par cette porte dérobée. Si la mise à jour immédiate n'est pas possible, isoler le service du réseau exposé. Vérifier l'absence de compromission antérieure sur le système. Restreindre l'accès au port 21 aux seules sources légitimes.

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-002 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

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 Apache 2.4.29 détecté sur NET-B-H1:80 est vulnérable à des failles de traversée de chemin (CVE-2021-41773, CVE-2021-42013). Ces vulnérabilités permettent de lire des fichiers arbitraires et potentiellement d'exécuter du code.

IMPACT

Un attaquant peut accéder à des fichiers sensibles du serveur ou exécuter du code arbitraire, 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>
```

VÉRIFICATION

Rejouer le plugin Nessus 156032 sur NET-B-H1 ; nmap -p80 -sV --script vulners NET-B-H1.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour Apache vers une version corrigée (2.4.51 ou ultérieure). Vérifier la configuration des alias et des permissions de fichiers. Contrôler les journaux d'accès pour détecter une exploitation antérieure.

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>

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

F-003 Fortinet FortiOS 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-2018-13379 Sources: NESSUS, NMAP

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-H2:443

L'équipement Fortinet FortiOS 6.0.4 exposé sur NET-B-H2:443 présente une vulnérabilité de traversée de chemin (CVE-2018-13379). Cette faille permet la lecture de fichiers système, notamment des identifiants de session.

IMPACT

Un attaquant peut récupérer des informations d'authentification et accéder au VPN ou à l'infrastructure protégée par cet équipement.

PREUVE

Installed version : 6.0.4

```
<port protocol="tcp" portid="443">
  <state state="open" reason="syn-ack"/>
  <service name="https" product="Fortinet SSL VPN" version="6.0.4" method="probed" conf="10"/>
</port>
```

VÉRIFICATION

Rejouer le plugin Nessus 111674 sur NET-B-H2 ; nmap -p443 -sV --script vulners NET-B-H2.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour FortiOS vers une version corrigée. Révoquer et renouveler les identifiants et sessions potentiellement exposés. Vérifier les journaux d'accès VPN pour détecter une exploitation antérieure.

RÉFÉRENCES

<https://nvd.nist.gov/vuln/detail/CVE-2018-13379>

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

<https://www.tenable.com/plugins/nessus/111674>

Contrôles rattachés: A.8.24, A.8.8, A.8.28, A.8.26, 21.2.e, 21.2.h, 21.2.j · Statut: Ouvert

Plan de remédiation

Immédiat (priorité 1)

Ce plan de remédiation hiérarchise les actions selon leur criticité et leur urgence opérationnelle. Onze findings critiques et élevés nécessitent une correction sans délai : accès non authentifiés à MongoDB, Redis et Elasticsearch, comptes par défaut ou sans mot de passe sur MySQL et PostgreSQL, backdoor vsftpd, vulnérabilités Apache, FortiOS et OpenSSL, ainsi que MS17-010 et l'accès anonyme Jenkins. Ces expositions permettent un accès direct aux données ou au système sans authentification et doivent être fermées ou corrigées en priorité 1.

F-001 — vsftpd Smiley Face Backdoor
F-002 — Apache 2.4.x < 2.4.51 Path Traversal
F-003 — Fortinet FortiOS Path Traversal
F-004 — MongoDB Unauthenticated Access
F-005 — MySQL Unpassworded Account Check
F-006 — OpenSSL 3.0.0 < 3.0.7 Buffer Overflow
F-007 — PostgreSQL Default Credentials
F-008 — Redis Server Unprotected Access
F-010 — MS17-010 SMB Remote Code Execution
F-011 — Elasticsearch Unauthenticated Access
F-012 — Jenkins Anonymous Access Enabled

À planifier (priorité 2)

Quatre findings de sévérité élevée sont à intégrer au cycle de correction courant : mise à jour de Jenkins, sécurisation du service SMTP contre l'injection en clair via STARTTLS, remplacement du certificat SSL non fiable, et désactivation du service Telnet non chiffré. Ces éléments ne présentent pas le même niveau d'urgence que le volet immédiat mais doivent être traités sans report excessif.

F-009 — Jenkins < 2.235.2 Multiple Vulnerabilities
F-013 — SMTP Service STARTTLS Plaintext Injection
F-014 — SSL Certificate Cannot Be Trusted
F-015 — Unencrypted Telnet Server

À surveiller (priorité 3)

Les findings de sévérité moyenne, faible ou informative peuvent être surveillés sans action immédiate : énumération d'utilisateurs OpenSSH, algorithmes SSH faibles, suites de chiffrement SSL de force moyenne, absence de NLA sur les services Terminal Server, méthodes HTTP TRACE/TRACK, protocole TLS 1.0, ainsi que les observations d'exposition de faible sévérité. Ces points sont à intégrer dans les prochains cycles de durcissement ou de mise à jour planifiée.

F-016 — OpenSSH < 7.9 User Enumeration
F-017 — SSH Weak Algorithms Supported
F-018 — SSL Medium Strength Cipher Suites Supported
F-019 — Terminal Services Doesn't Use NLA
F-020 — HTTP TRACE / TRACK Methods Allowed
F-021 — TLS Version 1.0 Protocol Detection
F-022 — Observations de sévérité faible — exposition d'informations

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-001, F-004, F-008, F-022
A.8.20	Networks security	F-010, F-016, F-017
A.8.21	Security of network services	F-001, F-015, F-019
A.8.22	Segregation of networks	F-005, F-007, F-010, F-016, F-017
A.8.24	Use of cryptography	F-003, F-006, F-013, F-014, F-018, F-021
A.8.26	Application security requirements	F-002, F-003, F-009, F-010, F-011, F-013, F-020
A.8.28	Secure coding	F-002, F-003, F-009, F-010, F-011, F-013, F-020
A.8.3	Information access restriction	F-001, F-004, F-005, F-007, F-008, F-022
A.8.5	Secure authentication	F-001, F-007, F-012, F-015, F-019
A.8.8	Management of technical vulnerabilities	F-001, F-002, F-003, F-006, F-009, F-010, F-013, F-016
A.8.9	Configuration management	F-012

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-006, F-008, F-009, F-010, F-011, F-013, F-016, F-020, F-022
21.2.f	Policies to assess the effectiveness of cybersecurity risk-management measures	F-012
21.2.g	Basic cyber hygiene practices and cybersecurity training	F-012
21.2.h	Policies on the use of cryptography and, where appropriate, encryption	F-003, F-006, F-013, F-014, F-018, F-021
21.2.i	Human resources security, access control policies and asset management	F-001, F-004, F-005, F-007, F-008, F-012, F-016, F-017, F-

		022
21.2.j	Use of multi-factor authentication, secured communications and secured emergency communication systems	F-003, F-006, F-007, F-012, F-013, F-014, F-016, F-017, F-018, F-021

Annexe technique

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	ACTIFS
F-001	vsftpd Smiley Face Backdoor	CRITIQUE	10.0	1
F-002	Apache 2.4.x < 2.4.51 Path Traversal	CRITIQUE	9.8	1
F-003	Fortinet FortiOS Path Traversal	CRITIQUE	9.8	1
F-004	MongoDB Unauthenticated Access	CRITIQUE	9.8	1
F-005	MySQL Unpassworded Account Check	CRITIQUE	9.8	1
F-006	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITIQUE	9.8	1
F-007	PostgreSQL Default Credentials	CRITIQUE	9.8	1
F-008	Redis Server Unprotected Access	CRITIQUE	9.8	1
F-009	Jenkins < 2.235.2 Multiple Vulnerabilities	ÉLEVÉE	8.8	1
F-010	MS17-010 SMB Remote Code Execution	ÉLEVÉE	8.1	1
F-011	Elasticsearch Unauthenticated Access	ÉLEVÉE	7.5	1
F-012	Jenkins Anonymous Access Enabled	ÉLEVÉE	7.5	1
F-013	SMTP Service STARTTLS Plaintext Injection	ÉLEVÉE	7.5	1
F-014	SSL Certificate Cannot Be Trusted	ÉLEVÉE	7.5	1
F-015	Unencrypted Telnet Server	ÉLEVÉE	7.5	1
F-016	OpenSSH < 7.9 User Enumeration	MOYENNE	5.3	1
F-017	SSH Weak Algorithms Supported	MOYENNE	5.3	1
F-018	SSL Medium Strength Cipher Suites Supported	MOYENNE	5.3	2
F-019	Terminal Services Doesn't Use NLA	MOYENNE	5.3	1
F-020	HTTP TRACE / TRACK Methods Allowed	FAIBLE	3.7	1
F-021	TLS Version 1.0 Protocol Detection	FAIBLE	3.7	1
F-022	Observations de sévérité faible — exposition d'informations	INFO		4

Annexe — Re-test

À compléter lors du contrôle de remédiation.

RÉF	INTITULÉ	STATUT	DATE	VÉRIFICATION
F-001	vsftpd Smiley Face Backdoor	Ouvert		
F-002	Apache 2.4.x < 2.4.51 Path Traversal	Ouvert		
F-003	Fortinet FortiOS Path Traversal	Ouvert		
F-004	MongoDB Unauthenticated Access	Ouvert		
F-005	MySQL Unpassworded Account Check	Ouvert		
F-006	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	Ouvert		
F-007	PostgreSQL Default Credentials	Ouvert		
F-008	Redis Server Unprotected Access	Ouvert		
F-009	Jenkins < 2.235.2 Multiple Vulnerabilities	Ouvert		
F-010	MS17-010 SMB Remote Code Execution	Ouvert		
F-011	Elasticsearch Unauthenticated Access	Ouvert		
F-012	Jenkins Anonymous Access Enabled	Ouvert		
F-013	SMTP Service STARTTLS Plaintext Injection	Ouvert		
F-014	SSL Certificate Cannot Be Trusted	Ouvert		
F-015	Unencrypted Telnet Server	Ouvert		
F-016	OpenSSH < 7.9 User Enumeration	Ouvert		
F-017	SSH Weak Algorithms Supported	Ouvert		
F-018	SSL Medium Strength Cipher Suites Supported	Ouvert		
F-019	Terminal Services Doesn't Use NLA	Ouvert		
F-020	HTTP TRACE / TRACK Methods Allowed	Ouvert		
F-021	TLS Version 1.0 Protocol Detection	Ouvert		
F-022	Observations de sévérité faible — exposition d'informations	Ouvert		