

CABINET DÉMO

Audit externe

Rapport d'audit de sécurité

PRÉPARÉ PAR	Cabinet Démo
-------------	--------------

DATE	05/08/2026
------	------------

PÉRIMÈTRE	Périmètre Internet
-----------	--------------------

Tableau de bord exécutif

15 VULNÉRABILITÉS	4 CRITIQUES	4 ÉLEVÉES
7 ACTIFS CONCERNÉS	8.5 CVSS MOYEN	3 À DISTANCE / SANS AUTHENTIFICATION

87 /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 4 · MOYENNE 1 · FAIBLE 2 · INFO 4
-----------------------------------	---

Impact métier

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

F-001 Apache 2.4.49/2.4.50 path traversal Un attaquant peut accéder à des fichiers sensibles du serveur ou exécuter du code arbitraire, entraînant une compromission complète du service web. NET-A-H1:80
F-002 FortiOS SSL VPN path traversal Un attaquant peut récupérer des identifiants VPN et obtenir un accès non autorisé au réseau interne de l'entreprise. NET-A-H2:443
F-003 Jenkins unauthenticated dashboard Un attaquant peut exécuter des jobs de build arbitraires et obtenir une exécution de code sur le serveur d'intégration continue, avec un impact potentiel sur l'ensemble de la chaîne de déploiement. NET-B-H1:8080

Chemin d'attaque

PRISE DE PIED	F-001 Apache 2.4.49/2.4.50 path traversal NET-A-H1:80 Sans authentification
ÉLEVATION	F-002 FortiOS SSL VPN path traversal NET-A-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 5 FINDINGS

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

Responsable: Ingénierie sécurité · Charge: Moyenne
F-001, F-002, F-003, F-004, F-005

Phase 2 COURT TERME · 8-30 JOURS 5 FINDINGS

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

Responsable: Administration système · Charge: Moyenne
F-006, F-007, F-008, F-009, F-011

Phase 3 MOYEN TERME · 31-90 JOURS 5 FINDINGS

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

Responsable: Ingénierie sécurité · Charge: Moyenne
F-010, F-012, F-013, F-014, F-015

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 systèmes exposés de l'entreprise, incluant serveurs web, VPN, outils d'intégration continue et bases de données. Plusieurs failles critiques ont été identifiées, certaines pouvant permettre à un attaquant externe de prendre le contrôle de serveurs ou d'accéder au réseau interne. Des accès non protégés et des identifiants par défaut aggravent l'exposition globale. Une action corrective rapide est nécessaire sur les points les plus critiques avant qu'ils ne soient exploités. Une décision de priorisation budgétaire et opérationnelle est recommandée pour traiter ces risques dans les meilleurs délais.

Risques majeurs

- Un accès non autorisé au réseau interne via le VPN pourrait compromettre l'ensemble du système d'information de l'entreprise.
- Une prise de contrôle des serveurs web, de la chaîne de déploiement ou des bases de données pourrait interrompre les activités et exposer des données sensibles de clients ou de l'entreprise.
- La divulgation de fichiers de configuration ou d'identifiants par défaut pourrait faciliter des attaques en cascade sur d'autres systèmes de l'entreprise.

Répartition par sévérité

SÉVÉRITÉ	#	%	
CRITIQUE	4	27%	
ÉLEVÉE	4	27%	
MOYENNE	1	7%	
FAIBLE	2	13%	
INFO	4	27%	

Périmètre et méthodologie

Dans le périmètre

Périmètre Internet

7 host(s)

NET-A-H1, NET-A-H2, NET-B-H1, NET-A-H3, NET-C-H1, NET-A-H4, NET-B-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
nuclei-engagement.jsonl	NUCLEI	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	Apache 2.4.49/2.4.50 path traversal	CRITIQUE	9.8	1	Ouvert
F-002	FortiOS SSL VPN path traversal	CRITIQUE	9.8	1	Ouvert
F-003	Jenkins unauthenticated dashboard	CRITIQUE	9.8	1	Ouvert
F-004	Redis unauthenticated access	CRITIQUE	9.8	1	Ouvert
F-005	Tomcat manager default credentials	ÉLEVÉE	8.8	1	Ouvert
F-006	vulners findings on port 445	ÉLEVÉE	8.1	2	Ouvert
F-007	Elasticsearch unauthenticated	ÉLEVÉE	7.5	2	Ouvert
F-008	Exposed .env file	ÉLEVÉE	7.5	2	Ouvert
F-009	vulners findings on port 22	MOYENNE	5.3	2	Ouvert
F-010	MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)	INFO		3	Ouvert
F-011	TELNET service exposed on port 23 (Linux telnetd)	INFO		2	Ouvert
F-012	Observations de sévérité faible — exposition d'informations	FAIBLE		3	Ouvert
F-013	Observations de sévérité faible — chiffrement TLS	FAIBLE		3	Ouvert
F-014	Observations de sévérité faible — bases de données	INFO		3	Ouvert
F-015	Observations de sévérité faible — services web	INFO		3	Ouvert

Findings — détail

Extrait : 3 findings sur 15 sont détaillés ci-dessous. Les 12 findings restants, leurs preuves et leur plan de remédiation figurent dans le rapport complet.

F-001 Apache 2.4.49/2.4.50 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: 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-A-H1:80

Le serveur Apache exposé sur NET-A-H1:80 présente une vulnérabilité de traversée de chemin (path traversal) identifiée par les CVE-2021-41773 et CVE-2021-42013. Cette faille permet de lire des fichiers arbitraires du serveur et, dans certains cas, d'exécuter du code à distance. La détection a été confirmée par nmap et nuclei.

IMPACT

Un attaquant peut accéder à des fichiers sensibles du serveur ou exécuter du code arbitraire, entraînant une compromission complète du service web.

PREUVE

```
<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-A-H1/cgi-bin/.%2e/%2e%2e/etc/passwd

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

VÉRIFICATION

Pour vérifier : exécuter nmap -p80 -sV --script vulners NET-A-H1 puis nuclei -id CVE-2021-41773 -u http://NET-A-H1.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour Apache vers une version corrigée immédiatement. Vérifier les logs d'accès à la recherche de tentatives d'exploitation passées. Restreindre l'accès au serveur via un pare-feu applicatif en attendant le correctif. Revalider la configuration des chemins exposés.

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://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

F-002 FortiOS SSL VPN path traversal

CRITIQUE CVSS 9.8 CWE-22 CVE-2018-13379 Sources: NMAP, NUCLEI

Sévérité critical : score CVSS de 9.8.

NET-A-H2:443

L'interface SSL VPN FortiOS exposée sur NET-A-H2:443 est vulnérable à une traversée de chemin référencée CVE-2018-13379. Cette vulnérabilité permet de lire des fichiers système, notamment des identifiants de session VPN.

IMPACT

Un attaquant peut récupérer des identifiants VPN et obtenir un accès non autorisé au réseau interne de l'entreprise.

PREUVE

```
<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>
```

Template: CVE-2018-13379

Matched at: https://NET-A-H2/remote/fgt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession

VÉRIFICATION

Pour vérifier : exécuter `nmap -p443 -sV --script vulners NET-A-H2` puis `nuclei -id CVE-2018-13379 -u https://NET-A-H2`.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Mettre à jour FortiOS vers une version corrigée sans délai. Forcer la réinitialisation des identifiants et sessions VPN existants. Limiter l'exposition de l'interface d'administration à des IP de confiance. Surveiller les connexions VPN pour détecter des accès suspects.

RÉFÉRENCES

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

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

<https://github.com/projectdiscovery/nuclei-templates/search?q=CVE-2018-13379>

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

F-003 Jenkins unauthenticated dashboard

CRITIQUE CVSS 9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-306 Sources: 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-H1:8080

Le tableau de bord Jenkins accessible sur NET-B-H1:8080 ne requiert pas d'authentification. Cette absence de contrôle d'accès a été confirmée par nmap et nuclei.

IMPACT

Un attaquant peut exécuter des jobs de build arbitraires et obtenir une exécution de code sur le serveur d'intégration continue, avec un impact potentiel sur l'ensemble de la chaîne de déploiement.

PREUVE

```
<port protocol="tcp" portid="8080">
  <state state="open" reason="syn-ack"/>
  <service name="http" product="Jenkins" version="2.222.1" method="probed" conf="10"/>
</port>
```

Template:jenkins-unauthenticated

Matched at: <http://NET-B-H1:8080/>

VÉRIFICATION

Pour vérifier : exécuter `nmap -p8080 -sV --script vulners NET-B-H1` puis `nuclei -id jenkins-unauthenticated -u http://NET-B-H1:8080`.

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Activer l'authentification et le contrôle d'accès sur Jenkins immédiatement. Restreindre l'accès réseau à l'interface d'administration. Auditer les jobs et plugins existants pour détecter toute modification non autorisée.

RÉFÉRENCES

<https://cwe.mitre.org/data/definitions/306.html>

<https://github.com/projectdiscovery/nuclei-templates/search?q=jenkins-unauthenticated>

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

Plan de remédiation

Immédiat (priorité 1)

Ce plan de remédiation présente les actions à mener selon trois niveaux de priorité, sans échéance chiffrée imposée. Cinq findings critiques ou élevés nécessitent un traitement sans attendre : la faille de traversée de répertoire sur Apache (F-001), la vulnérabilité de path traversal sur FortiOS SSL VPN (F-002), le tableau de bord Jenkins accessible sans authentification (F-003), l'accès Redis non authentifié (F-004) et les identifiants par défaut sur Tomcat manager (F-005). Ces expositions permettent un accès non contrôlé à des services sensibles et doivent être corrigées en priorité 1. Aucune de ces vulnérabilités n'est référencée au catalogue KEV selon les données fournies, mais leur sévérité justifie une action immédiate.

F-001 — Apache 2.4.49/2.4.50 path traversal

F-002 — FortiOS SSL VPN path traversal

F-003 — Jenkins unauthenticated dashboard

F-004 — Redis unauthenticated access

F-005 — Tomcat manager default credentials

À planifier (priorité 2)

Le cycle courant doit intégrer le traitement de cinq findings de priorité 2. Il s'agit des résultats vulners sur le port 445 (F-006), de l'exposition Elasticsearch non authentifiée (F-007), du fichier .env exposé (F-008), des résultats vulners sur le port 22 (F-009) et du service TELNET exposé sur le port 23 (F-011). Ces éléments présentent des niveaux de sévérité élevés à informatifs et doivent être planifiés dans le cycle de remédiation en cours.

F-006 — vulners findings on port 445

F-007 — Elasticsearch unauthenticated

F-008 — Exposed .env file

F-009 — vulners findings on port 22

F-011 — TELNET service exposed on port 23 (Linux telnetd)

À surveiller (priorité 3)

Cinq findings de priorité 3 sont à surveiller sans nécessiter d'action immédiate. Le service RDP exposé sur le port 3389 (F-010) ainsi que les observations de faible sévérité relatives à l'exposition (F-012), au TLS (F-013), à la base de données (F-014) et au web (F-015) relèvent de ce niveau. Ces éléments sont de sévérité faible ou informative et ne présentent pas, selon les données disponibles, d'indicateur d'exploitabilité renforcée.

F-010 — MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)

F-012 — Observations de sévérité faible — exposition d'informations

F-013 — Observations de sévérité faible — chiffrement TLS

F-014 — Observations de sévérité faible — bases de données

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

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-007, F-009, F-012, F-015
21.2.f	Policies to assess the effectiveness of cybersecurity risk-management measures	F-005
21.2.g	Basic cyber hygiene practices and cybersecurity training	F-005
21.2.h	Policies on the use of cryptography and, where appropriate, encryption	F-002, F-008, F-013
21.2.i	Human resources security, access control policies and asset management	F-004, F-005, F-009, F-012, F-014
21.2.j	Use of multi-factor authentication, secured communications and secured emergency communication systems	F-002, F-005, F-008, F-009, F-013

Annexe technique

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	ACTIFS
F-001	Apache 2.4.49/2.4.50 path traversal	CRITIQUE	9.8	1
F-002	FortiOS SSL VPN path traversal	CRITIQUE	9.8	1
F-003	Jenkins unauthenticated dashboard	CRITIQUE	9.8	1
F-004	Redis unauthenticated access	CRITIQUE	9.8	1
F-005	Tomcat manager default credentials	ÉLEVÉE	8.8	1
F-006	vulners findings on port 445	ÉLEVÉE	8.1	1
F-007	Elasticsearch unauthenticated	ÉLEVÉE	7.5	1
F-008	Exposed .env file	ÉLEVÉE	7.5	2
F-009	vulners findings on port 22	MOYENNE	5.3	1
F-010	MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)	INFO		1
F-011	TELNET service exposed on port 23 (Linux telnetd)	INFO		1
F-012	Observations de sévérité faible — exposition d'informations	FAIBLE		8
F-013	Observations de sévérité faible — chiffrement TLS	FAIBLE		5
F-014	Observations de sévérité faible — bases de données	INFO		2
F-015	Observations de sévérité faible — services web	INFO		6

Annexe — Re-test

À compléter lors du contrôle de remédiation.

RÉF	INTITULÉ	STATUT	DATE	VÉRIFICATION
F-001	Apache 2.4.49/2.4.50 path traversal	Ouvert		
F-002	FortiOS SSL VPN path traversal	Ouvert		
F-003	Jenkins unauthenticated dashboard	Ouvert		
F-004	Redis unauthenticated access	Ouvert		
F-005	Tomcat manager default credentials	Ouvert		
F-006	vulners findings on port 445	Ouvert		
F-007	Elasticsearch unauthenticated	Ouvert		
F-008	Exposed .env file	Ouvert		
F-009	vulners findings on port 22	Ouvert		
F-010	MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)	Ouvert		
F-011	TELNET service exposed on port 23 (Linux telnetd)	Ouvert		
F-012	Observations de sévérité faible — exposition d'informations	Ouvert		
F-013	Observations de sévérité faible — chiffrement TLS	Ouvert		
F-014	Observations de sévérité faible — bases de données	Ouvert		
F-015	Observations de sévérité faible — services web	Ouvert		