

CABINET DÉMO

External audit

Security assessment report

PREPARED BY	Cabinet Démo
-------------	--------------

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

SCOPE	Internet perimeter
-------	--------------------

Executive dashboard

15 VULNERABILITIES	4 CRITICAL	4 HIGH
7 AFFECTED ASSETS	8.5 AVERAGE CVSS	3 REMOTE / UNAUTHENTICATED

87

/100
RISK SCORE

OVERALL POSTURE

Critical exposure

The score is a weighted exposure index (0 = contained, 100 = critical) derived from severity, CVSS and exploitability. It measures no form of compliance.

SEVERITY DISTRIBUTION

CRITICAL 4 · HIGH 4 · MEDIUM 1 · LOW 2 · INFO 4

Business impact

Concrete consequences for the business if the major exposures are left untreated.

F-001 Apache 2.4.49/2.4.50 path traversal
Successful exploitation can lead to full server compromise, disclosure of sensitive files, and unauthorized access to internal systems reachable from this host. NET-A-H1:80
F-002 FortiOS SSL VPN path traversal
An attacker exploiting this flaw could retrieve VPN session credentials and gain unauthorized remote access to the internal network. NET-A-H2:443
F-003 Jenkins unauthenticated dashboard
An unauthenticated attacker could access build configurations, credentials stored in Jenkins, and potentially execute arbitrary code on the underlying host via job configuration. NET-B-H1:8080

Attack path

FOOTHOLD	F-001 Apache 2.4.49/2.4.50 path traversal NET-A-H1:80 Unauthenticated
ESCALATION	F-002 FortiOS SSL VPN path traversal NET-A-H2:443 Code execution
BUSINESS IMPACT	Data loss, service interruption and regulatory exposure.

The most plausible chain from external access to business impact, based on the findings above. Stages not supported by a finding are not shown.

Remediation roadmap

Phase 1

IMMEDIATE · 0-7 DAYS

5 FINDINGS

Contain remote code execution and unauthenticated access.

Owner: Security engineering · Effort: Medium
F-001, F-002, F-003, F-004, F-005

Phase 2 SHORT TERM · 8-30 DAYS 5 FINDINGS

Fix high-severity services and remove weak credentials.

Owner: Systems administration · Effort: Medium
F-006, F-007, F-008, F-009, F-011

Phase 3 MEDIUM TERM · 31-90 DAYS 5 FINDINGS

Harden configuration, TLS and monitoring; retest the scope.

Owner: Security engineering · Effort: Medium
F-010, F-012, F-013, F-014, F-015

Document control

VERSION	1.0
DATE	05/08/2026
AUTHOR	Cabinet Démo
CLASSIFICATION	Confidential — restricted distribution
DISTRIBUTION	Client and issuing firm; do not redistribute without written consent.
CONTACT	Not provided

Executive summary

L'audit a couvert un ensemble de systèmes exposés incluant des serveurs web, une passerelle VPN, un outil d'intégration logicielle, des bases de données et des services applicatifs internes. Plusieurs failles critiques ont été identifiées, permettant à un attaquant d'accéder sans autorisation à des systèmes internes, de récupérer des données sensibles ou d'exécuter des actions à distance sur certains serveurs. Ces faiblesses résultent notamment de logiciels non mis à jour, de services laissés accessibles sans authentification, et d'identifiants par défaut non modifiés. Une action de remédiation rapide est recommandée sur les points critiques afin de réduire l'exposition de l'entreprise. Une décision doit être prise sur la priorisation et le calendrier de correction, en particulier pour les accès distants et les services exposés sur Internet.

Top risks

- Un accès non autorisé au réseau interne de l'entreprise via la passerelle d'accès distant pourrait permettre à un attaquant de contourner les contrôles de sécurité périmétriques.
- La compromission de serveurs exposés pourrait entraîner un vol ou une destruction de données sensibles, avec un impact direct sur la continuité des activités et la réputation de l'entreprise.
- Des identifiants par défaut et des services non protégés augmentent le risque qu'un attaquant obtienne un accès complet à des systèmes critiques sans effort technique particulier.

Severity distribution

SEVERITY	#	%	
CRITICAL	4	27%	
HIGH	4	27%	
MEDIUM	1	7%	
LOW	2	13%	
INFO	4	27%	

Scope and methodology

In scope

Internet perimeter

7 host(s)

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

Out of scope

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

Files analysed

FILE	DETECTED TOOL	STATE
nmap-engagement.xml	NMAP	Parsed
nuclei-engagement.jsonl	NUCLEI	Parsed

Methodology and limitations

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.

No external enrichment could be applied (CISA KEV and EPSS unavailable): ratings rest on CVSS and the severities reported by the tools alone.

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.

Rating and prioritisation method

Severity scale

SEVERITY	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

Applied adjustments

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.

Priority meanings

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

Findings summary

REF	TITLE	SEVERITY	CVSS	PRIORITY	STATUS
F-001	Apache 2.4.49/2.4.50 path traversal	CRITICAL	9.8	1	Open
F-002	FortiOS SSL VPN path traversal	CRITICAL	9.8	1	Open
F-003	Jenkins unauthenticated dashboard	CRITICAL	9.8	1	Open
F-004	Redis unauthenticated access	CRITICAL	9.8	1	Open
F-005	Tomcat manager default credentials	HIGH	8.8	1	Open
F-006	vulners findings on port 445	HIGH	8.1	2	Open
F-007	Elasticsearch unauthenticated	HIGH	7.5	2	Open
F-008	Exposed .env file	HIGH	7.5	2	Open
F-009	vulners findings on port 22	MEDIUM	5.3	2	Open
F-010	MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)	INFO		3	Open
F-011	TELNET service exposed on port 23 (Linux telnetd)	INFO		2	Open
F-012	Low-severity observations — information exposure	LOW		3	Open
F-013	Low-severity observations — TLS encryption	LOW		3	Open
F-014	Low-severity observations — databases	INFO		3	Open
F-015	Low-severity observations — web services	INFO		3	Open

Findings — detail

Extract: 3 of 15 findings are written up below. The remaining 12, their evidence and the remediation plan are in the full report.

F-001 Apache 2.4.49/2.4.50 path traversal

CRITICAL 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.

CVSS detail — Attack vector: Network · Complexity: Low · Privileges required: None · User interaction: None · Scope: Unchanged · Confidentiality: High · Integrity: High · Availability: High

AFFECTED ASSETS

NET-A-H1:80

The Apache httpd instance exposed on NET-A-H1:80 is affected by known path traversal vulnerabilities CVE-2021-41773 and CVE-2021-42013. These flaws allow an attacker to access files outside the web root and, under certain configurations, execute arbitrary code via CGI.

IMPACT

Successful exploitation can lead to full server compromise, disclosure of sensitive files, and unauthorized access to internal systems reachable from this host.

EVIDENCE

```
<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

VERIFICATION

To verify: run `nmap -p80 -sV --script vulners NET-A-H1` and `nuclei -id CVE-2021-41773 -u http://NET-A-H1`.

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade Apache httpd to a version not affected by CVE-2021-41773 and CVE-2021-42013. Disable CGI execution where not strictly required. Restrict access to the web root and review logs for signs of prior exploitation attempts.

REFERENCES

<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>

Mapped controls: A.8.8, A.8.26, A.8.28, 21.2.e · Status: Open

F-002 FortiOS SSL VPN path traversal

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

Sévérité critical : score CVSS de 9.8.

AFFECTED ASSETS

NET-A-H2:443

The FortiOS SSL VPN service on NET-A-H2:443 is affected by CVE-2018-13379, a path traversal vulnerability allowing unauthenticated retrieval of system files, including session data.

IMPACT

An attacker exploiting this flaw could retrieve VPN session credentials and gain unauthorized remote access to the internal network.

EVIDENCE

```
<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

VERIFICATION

To verify: run `nmap -p443 -sV --script vulners NET-A-H2` and `nuclei -id CVE-2018-13379 -u https://NET-A-H2`.

REMIEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade the FortiOS version to a release that addresses CVE-2018-13379. Rotate VPN credentials and session secrets after remediation. Review VPN access logs for anomalous connections.

REFERENCES

<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>

Mapped controls: A.8.24, A.8.8, A.8.28, A.8.26, 21.2.e, 21.2.h, 21.2.j · Status: Open

F-003 Jenkins unauthenticated dashboard

CRITICAL 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.

CVSS detail — Attack vector: Network · Complexity: Low · Privileges required: None · User interaction: None · Scope: Unchanged · Confidentiality: High · Integrity: High · Availability: High

AFFECTED ASSETS

NET-B-H1:8080

A Jenkins instance on NET-B-H1:8080 is reachable without authentication, exposing its administrative dashboard to any network client.

IMPACT

An unauthenticated attacker could access build configurations, credentials stored in Jenkins, and potentially execute arbitrary code on the underlying host via job configuration.

EVIDENCE

```
<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/>

VERIFICATION

To verify: run `nmap -p8080 -sV --script vulners NET-B-H1` and `nuclei -id jenkins-unauthenticated -u http://NET-B-H1:8080`.

REMIEDIATION — PRIORITY 1 (IMMEDIATE)

Enable authentication and authorization on the Jenkins instance immediately. Restrict network access to the Jenkins port to trusted hosts. Review existing jobs and credentials for signs of unauthorized modification.

REFERENCES

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

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

Mapped controls: A.8.26, A.8.28, 21.2.e · Status: Open

Remediation roadmap

Immediate (priority 1)

This plan organizes remediation into three priority tiers based on the findings identified during the assessment. Five critical/high findings require immediate attention: Apache 2.4.49/2.4.50 path traversal (F-001), FortiOS SSL VPN path traversal (F-002), Jenkins unauthenticated dashboard (F-003), Redis unauthenticated access (F-004), and Tomcat manager default credentials (F-005). These expose services to unauthenticated access or path traversal without further conditions. They should be patched, reconfigured with authentication, or restricted from network exposure as a priority.

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

Planned (priority 2)

Five findings should be scheduled within the current remediation cycle: vulners findings on port 445 (F-006), Elasticsearch unauthenticated (F-007), exposed .env file (F-008), vulners findings on port 22 (F-009), and TELNET service exposed on port 23 (F-011). These findings range from high to informational severity and involve exposed services or configuration data that should be addressed through access restriction, patching, or service hardening. None are flagged as actively exploited (kev: false).

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)

Monitor (priority 3)

Five low/informational findings can be tracked without immediate action: MS-WBT-SERVER service exposed on port 3389 (F-010), and observations of low severity related to exposure (F-012), TLS (F-013), database (F-014), and web (F-015). These do not require urgent remediation but should be reviewed periodically to confirm no change in risk level.

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

F-012 — Low-severity observations — information exposure

F-013 — Low-severity observations — TLS encryption

F-014 — Low-severity observations — databases

F-015 — Low-severity observations — web services

Annex — Control mapping

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

Technical annex

REF	TITLE	SEVERITY	CVSS	ASSETS
F-001	Apache 2.4.49/2.4.50 path traversal	CRITICAL	9.8	1
F-002	FortiOS SSL VPN path traversal	CRITICAL	9.8	1
F-003	Jenkins unauthenticated dashboard	CRITICAL	9.8	1
F-004	Redis unauthenticated access	CRITICAL	9.8	1
F-005	Tomcat manager default credentials	HIGH	8.8	1
F-006	vulners findings on port 445	HIGH	8.1	1
F-007	Elasticsearch unauthenticated	HIGH	7.5	1
F-008	Exposed .env file	HIGH	7.5	2
F-009	vulners findings on port 22	MEDIUM	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	Low-severity observations — information exposure	LOW		8
F-013	Low-severity observations — TLS encryption	LOW		5
F-014	Low-severity observations — databases	INFO		2
F-015	Low-severity observations — web services	INFO		6

Annex — Re-test

To be completed during remediation verification.

REF	TITLE	STATUS	DATE	VERIFICATION
F-001	Apache 2.4.49/2.4.50 path traversal	Open		
F-002	FortiOS SSL VPN path traversal	Open		
F-003	Jenkins unauthenticated dashboard	Open		
F-004	Redis unauthenticated access	Open		
F-005	Tomcat manager default credentials	Open		
F-006	vulners findings on port 445	Open		
F-007	Elasticsearch unauthenticated	Open		
F-008	Exposed .env file	Open		
F-009	vulners findings on port 22	Open		
F-010	MS-WBT-SERVER service exposed on port 3389 (Microsoft Terminal Services)	Open		
F-011	TELNET service exposed on port 23 (Linux telnetd)	Open		
F-012	Low-severity observations — information exposure	Open		
F-013	Low-severity observations — TLS encryption	Open		
F-014	Low-severity observations — databases	Open		
F-015	Low-severity observations — web services	Open		