

CABINET DÉMO

Internal network test

Security assessment report

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

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

SCOPE	Internal segment
-------	------------------

Executive dashboard

22 VULNERABILITIES	8 CRITICAL	7 HIGH
7 AFFECTED ASSETS	7.7 AVERAGE CVSS	5 REMOTE / UNAUTHENTICATED

98

/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 8 · HIGH 7 · MEDIUM 4 · LOW 2 · INFO 1

Business impact

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

F-001 vsftpd Smiley Face Backdoor An attacker could gain remote command execution on the host, leading to full compromise of the system and potential lateral movement within the network. NET-A-H1:21
F-002 Apache 2.4.x < 2.4.51 Path Traversal An attacker could read arbitrary files or execute code on the server, potentially exposing sensitive data or compromising the web application. NET-B-H1:80
F-003 Fortinet FortiOS Path Traversal An attacker could retrieve session files containing credentials, enabling unauthorized access to the VPN and internal network resources. NET-B-H2:443

Attack path

FOOTHOLD	F-002 Apache 2.4.x < 2.4.51 Path Traversal
ESCALATION	NET-B-H1:80 Unauthenticated F-003 Fortinet FortiOS Path Traversal
BUSINESS IMPACT	NET-B-H2:443 Code execution 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 10 FINDINGS

Contain remote code execution and unauthenticated access.

Owner: Security engineering · Effort: High
F-001, F-002, F-003, F-004, F-005, F-006 ...

Phase 2 SHORT TERM · 8-30 DAYS 8 FINDINGS

Fix high-severity services and remove weak credentials.

Owner: Security engineering · Effort: Medium
F-011, F-012, F-013, F-014, F-015, F-017 ...

Phase 3 MEDIUM TERM · 31-90 DAYS 4 FINDINGS

Harden configuration, TLS and monitoring; retest the scope.

Owner: Security engineering · Effort: Medium
F-016, F-020, F-021, F-022

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 porté sur un ensemble de systèmes exposés incluant des serveurs web, des bases de données, des services d'infrastructure et un outil de gestion de développement logiciel. Il révèle un nombre élevé de failles critiques touchant des services accessibles sans authentification correcte ou protégés par des identifiants par défaut. Ces failles permettraient à un attaquant d'accéder aux données de l'entreprise, de les modifier ou de les détruire, et dans plusieurs cas de prendre le contrôle complet des systèmes concernés. Aucune de ces vulnérabilités n'est actuellement signalée comme exploitée activement dans la nature, mais leur nombre et leur nature indiquent une exposition significative. Une décision rapide est nécessaire pour prioriser la remédiation des accès non protégés et des systèmes obsolètes avant qu'un incident ne survienne.

Top risks

- Perte ou vol de données sensibles stockées dans les bases de l'entreprise, en raison de plusieurs bases de données accessibles sans authentification suffisante.
- Interruption ou compromission des services informatiques critiques, plusieurs systèmes pouvant être totalement pris en main à distance par un attaquant.
- Atteinte à la confiance des clients et partenaires, notamment via des certificats non fiables et des communications non chiffrées pouvant exposer des échanges sensibles.

Severity distribution

SEVERITY	#	%	
CRITICAL	8	36%	
HIGH	7	32%	
MEDIUM	4	18%	
LOW	2	9%	
INFO	1	5%	

Scope and methodology

In scope

Internal segment

7 host(s)

NET-A-H1, NET-B-H1, NET-B-H2, NET-C-H1, NET-B-H3, NET-B-H4, NET-C-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
nessus-engagement.nessus	NESSUS	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	vsftpd Smiley Face Backdoor	CRITICAL	10.0	1	Open
F-002	Apache 2.4.x < 2.4.51 Path Traversal	CRITICAL	9.8	1	Open
F-003	Fortinet FortiOS Path Traversal	CRITICAL	9.8	1	Open
F-004	MongoDB Unauthenticated Access	CRITICAL	9.8	1	Open
F-005	MySQL Unpassworded Account Check	CRITICAL	9.8	1	Open
F-006	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITICAL	9.8	1	Open
F-007	PostgreSQL Default Credentials	CRITICAL	9.8	1	Open
F-008	Redis Server Unprotected Access	CRITICAL	9.8	1	Open
F-009	Jenkins < 2.235.2 Multiple Vulnerabilities	HIGH	8.8	1	Open
F-010	MS17-010 SMB Remote Code Execution	HIGH	8.1	1	Open
F-011	Elasticsearch Unauthenticated Access	HIGH	7.5	2	Open
F-012	Jenkins Anonymous Access Enabled	HIGH	7.5	2	Open
F-013	SMTP Service STARTTLS Plaintext Injection	HIGH	7.5	2	Open
F-014	SSL Certificate Cannot Be Trusted	HIGH	7.5	2	Open
F-015	Unencrypted Telnet Server	HIGH	7.5	2	Open
F-016	OpenSSH < 7.9 User Enumeration	MEDIUM	5.3	3	Open
F-017	SSH Weak Algorithms Supported	MEDIUM	5.3	2	Open
F-018	SSL Medium Strength Cipher Suites Supported	MEDIUM	5.3	2	Open
F-019	Terminal Services Doesn't Use NLA	MEDIUM	5.3	2	Open
F-020	HTTP TRACE / TRACK Methods Allowed	LOW	3.7	3	Open
F-021	TLS Version 1.0 Protocol Detection	LOW	3.7	3	Open
F-022	Low-severity observations — information exposure	INFO		3	Open

Findings — detail

Extract: 3 of 22 findings are written up below. The remaining 19, their evidence and the remediation plan are in the full report.

F-001 vsftpd Smiley Face Backdoor

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

Sévérité critical : score CVSS de 10.0.

AFFECTED ASSETS

NET-A-H1:21

The FTP service on NET-A-H1:21 runs vsftpd 2.3.4, a version known to contain a backdoor allowing command execution. This version was flagged by both Nessus and Nmap during the scan.

IMPACT

An attacker could gain remote command execution on the host, leading to full compromise of the system and potential lateral movement within the network.

EVIDENCE

```
<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>
```

VERIFICATION

Re-run Nessus plugin 52703 against NET-A-H1; nmap -p21 -sV --script vulners NET-A-H1

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade vsftpd to a supported, patched version immediately. Verify the binary has not already been tampered with by comparing checksums against a trusted source. Restrict FTP access to trusted networks and disable the service if not required.

REFERENCES

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

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

Mapped controls: A.8.8, A.8.12, A.8.3, A.8.21, A.8.5, 21.2.e, 21.2.i · Status: Open

F-002 Apache 2.4.x < 2.4.51 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: NESSUS, NMAP

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-H1:80

The web server on NET-B-H1:80 runs Apache 2.4.29, which is affected by a path traversal vulnerability documented under CVE-2021-41773 and CVE-2021-42013. The installed version predates the fix released in 2.4.51.

IMPACT

An attacker could read arbitrary files or execute code on the server, potentially exposing sensitive data or compromising the web application.

EVIDENCE

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>
```

VERIFICATION

Re-run Nessus plugin 156032 against NET-B-H1; nmap -p80 -sV --script vulners NET-B-H1

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade Apache HTTP Server to a version 2.4.51 or later. Review server configuration for CGI and mod_cgi exposure. Check web logs for evidence of prior exploitation attempts targeting this path traversal pattern.

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

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

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

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-H2:443

The service on NET-B-H2:443 runs FortiOS 6.0.4, affected by a path traversal vulnerability referenced as CVE-2018-13379. This flaw allows unauthenticated access to system files via the SSL VPN interface.

IMPACT

An attacker could retrieve session files containing credentials, enabling unauthorized access to the VPN and internal network resources.

EVIDENCE

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>
```

VERIFICATION

Re-run Nessus plugin 111674 against NET-B-H2; nmap -p443 -sV --script vulners NET-B-H2

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade FortiOS to a patched version as recommended by the vendor. Rotate all credentials potentially exposed through this vulnerability. Review VPN access logs for signs of prior exploitation.

REFERENCES

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

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

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

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

Remediation roadmap

Immediate (priority 1)

Ce plan de remédiation organise les actions correctives en trois horizons de priorité. Les findings critiques et élevés (F-001 à F-010) exposent des services sans authentification ou avec des identifiants par défaut — vsftpd, Apache, FortiOS, MongoDB, MySQL, OpenSSL, PostgreSQL, Redis, Jenkins et SMB (MS17-010). Ces vulnérabilités doivent être corrigées sans délai, par mise à jour des composants concernés, désactivation des accès non authentifiés et remplacement des comptes par défaut. Aucune de ces failles n'est référencée comme exploitée activement (KEV) dans les données fournies, mais leur sévérité critique justifie un traitement immédiat.

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-009 — Jenkins < 2.235.2 Multiple Vulnerabilities
F-010 — MS17-010 SMB Remote Code Execution

Planned (priority 2)

Les findings de priorité 2 (F-011 à F-019) concernent des expositions de services (Elasticsearch, Jenkins en accès anonyme, Telnet en clair), des faiblesses de configuration TLS/SSH et l'absence de NLA sur les services Terminal Services. Ces éléments doivent être intégrés au cycle de correction courant, avec durcissement des configurations et remplacement des protocoles non chiffrés. Le certificat SSL non fiable (F-014) doit également être régularisé dans ce cycle.

F-011 — Elasticsearch Unauthenticated Access
F-012 — Jenkins Anonymous Access Enabled
F-013 — SMTP Service STARTTLS Plaintext Injection
F-014 — SSL Certificate Cannot Be Trusted
F-015 — Unencrypted Telnet Server
F-017 — SSH Weak Algorithms Supported
F-018 — SSL Medium Strength Cipher Suites Supported
F-019 — Terminal Services Doesn't Use NLA

Monitor (priority 3)

Les findings de priorité 3 (F-016, F-020 à F-022) sont de sévérité moyenne à faible ou informative : énumération d'utilisateurs OpenSSH, méthodes HTTP TRACE/TRACK, TLS 1.0 encore actif, et observations générales d'exposition. Ces points ne requièrent pas d'action immédiate mais doivent être suivis afin d'éviter leur accumulation ou leur combinaison avec d'autres faiblesses.

F-016 — OpenSSH < 7.9 User Enumeration
F-020 — HTTP TRACE / TRACK Methods Allowed
F-021 — TLS Version 1.0 Protocol Detection
F-022 — Low-severity observations — information exposure

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-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

Technical annex

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

Annex — Re-test

To be completed during remediation verification.

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