

CABINET DÉMO

ISO 27001 / NIS2 technical evidence

Security assessment report

PREPARED BY Cabinet Démo

DATE 05/08/2026

SCOPE Audited scope

Executive dashboard

40 VULNERABILITIES	13 CRITICAL	15 HIGH
9 AFFECTED ASSETS	8.0 AVERAGE CVSS	9 REMOTE / UNAUTHENTICATED

100 /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 13 · HIGH 15 · MEDIUM 9 · LOW 3
--	---

Business impact

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

F-001 CVE-2021-44228 in log4js 6.3.0
Exploitation could allow an attacker to compromise the application, potentially leading to unauthorized access to data processed by the API service. HOST-01
F-002 vsftpd Smiley Face Backdoor
If exploited, this issue could allow unauthorized remote access to the host, compromising confidentiality and integrity of data on the affected system. NET-A-H1:21
F-003 Apache 2.4.x < 2.4.51 Path Traversal
Exploitation could allow an attacker to read arbitrary files or execute code on the server, potentially exposing sensitive data or leading to further compromise of the host. NET-B-H1:80

Attack path

FOOTHOLD	F-001 CVE-2021-44228 in log4js 6.3.0 HOST-01 Unauthenticated
ESCALATION	F-003 Apache 2.4.x < 2.4.51 Path Traversal NET-B-H1:80 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 17 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 13 FINDINGS

Fix high-severity services and remove weak credentials.

Owner: Infrastructure & DevOps · Effort: High
F-014, F-015, F-016, F-019, F-020, F-021 ...

Phase 3 MEDIUM TERM · 31-90 DAYS 10 FINDINGS

Harden configuration, TLS and monitoring; retest the scope.

Owner: Infrastructure & DevOps · Effort: High
F-029, F-030, F-031, F-032, F-033, F-035 ...

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 serveurs, bases de données et services applicatifs exposés. Un nombre élevé de failles critiques a été identifié, touchant des composants d'infrastructure (bases de données, serveurs web, outils d'administration) ainsi que des bibliothèques logicielles utilisées par les applications. Plusieurs de ces failles concernent des accès non protégés ou des identifiants par défaut, ce qui facilite une exploitation. La direction doit décider d'un plan de remédiation prioritaire pour ces composants avant toute nouvelle mise en production ou exposition supplémentaire.

Top risks

- Des bases de données et interfaces d'administration accessibles sans authentification pourraient permettre le vol, la modification ou la destruction de données métier.
- Des vulnérabilités critiques dans des composants serveurs et bibliothèques logicielles pourraient permettre à un attaquant de prendre le contrôle de systèmes ou de services essentiels à l'activité.
- L'accumulation de failles critiques sur un périmètre limité augmente le risque d'interruption de service et d'atteinte à la réputation en cas d'incident de sécurité rendu public.

Severity distribution

SEVERITY	#	%	
CRITICAL	13	32%	
HIGH	15	38%	
MEDIUM	9	22%	
LOW	3	8%	
INFO	0	0%	

Scope and methodology

In scope

Audited scope

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

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
nuclei-engagement.jsonl	NUCLEI	Parsed
trivy-api-image.json	TRIVY	Parsed
trivy-worker-image.json	TRIVY	Parsed

Methodology and limitations

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.

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	CVE-2021-44228 in log4js 6.3.0	CRITICAL	10.0	1	Open
F-002	vsftpd Smiley Face Backdoor	CRITICAL	10.0	1	Open
F-003	Apache 2.4.x < 2.4.51 Path Traversal	CRITICAL	9.8	1	Open
F-004	CVE-2021-3711 in openssl 1.1.1k	CRITICAL	9.8	1	Open
F-005	CVE-2022-3602 in openssl 3.0.5-1	CRITICAL	9.8	1	Open
F-006	CVE-2022-37434 in zlib 1.2.12-r1	CRITICAL	9.8	1	Open
F-007	Fortinet FortiOS Path Traversal	CRITICAL	9.8	1	Open
F-008	Jenkins unauthenticated dashboard	CRITICAL	9.8	1	Open
F-009	MongoDB Unauthenticated Access	CRITICAL	9.8	1	Open
F-010	MySQL Unpassworded Account Check	CRITICAL	9.8	1	Open
F-011	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	CRITICAL	9.8	1	Open
F-012	PostgreSQL Default Credentials	CRITICAL	9.8	1	Open
F-013	Redis Server Unprotected Access	CRITICAL	9.8	1	Open
F-014	CVE-2022-28391 in busybox 1.35.0-r17	HIGH	8.8	2	Open
F-015	CVE-2023-38545 in curl 7.83.1-r3	HIGH	8.8	2	Open
F-016	Jenkins < 2.235.2 Multiple Vulnerabilities	HIGH	8.8	2	Open
F-017	Tomcat manager default credentials	HIGH	8.8	1	Open
F-018	MS17-010 SMB Remote Code Execution	HIGH	8.1	1	Open
F-019	CVE-2023-4911 in glibc 2.31-13	HIGH	7.8	2	Open
F-020	CVE-2022-3786 in openssl 3.0.5-1	HIGH	7.5	2	Open
F-021	CVE-2022-4450 in openssl 1.1.1q-r0	HIGH	7.5	2	Open
F-022	Elasticsearch Unauthenticated Access	HIGH	7.5	1	Open
F-023	Exposed .env file	HIGH	7.5	1	Open
F-024	SMTP Service STARTTLS Plaintext	HIGH	7.5	2	Open

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

Findings — detail

Extract: 3 of 40 findings are written up below. The remaining 37, their evidence and the remediation plan are in the full report.

F-001 CVE-2021-44228 in log4js 6.3.0

CRITICAL 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.

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

AFFECTED ASSETS

HOST-01

The api:1.4.2 container image includes log4js version 6.3.0, which is affected by CVE-2021-44228. Trivy identified a fixed version 6.4.0 that is not currently in use. This vulnerability is associated with CWE-502 (deserialization of untrusted data).

IMPACT

Exploitation could allow an attacker to compromise the application, potentially leading to unauthorized access to data processed by the API service.

EVIDENCE

```
Target: app/package-lock.json
Package: log4js
Installed version: 6.3.0
Fixed version: 6.4.0
Vulnerability: CVE-2021-44228
```

VERIFICATION

To verify, run: trivy image --severity HIGH,CRITICAL HOST-10/api:1.4.2

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade log4js to version 6.4.0 or later in the api:1.4.2 image. Rebuild and redeploy the container image after the update. Re-scan the image with Trivy to confirm the vulnerability is resolved. Integrate dependency scanning into the CI/CD pipeline to prevent recurrence.

REFERENCES

<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

<https://cwe.mitre.org/data/definitions/502.html>

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

F-002 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 was identified as vsftpd, associated with CVE-2011-2523, known as the vsftpd Smiley Face Backdoor. This finding was confirmed by both Nessus and Nmap.

IMPACT

If exploited, this issue could allow unauthorized remote access to the host, compromising confidentiality and integrity of data on the affected system.

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

To verify, re-run Nessus plugin 52703 against NET-A-H1 and run: `nmap -p21 -sV --script vulners NET-A-H1`

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Identify the vsftpd version in use on the host and upgrade to a version not affected by CVE-2011-2523. If the identified backdoor functionality is confirmed, rebuild the affected system from a trusted source. Restrict FTP service exposure to trusted networks where possible.

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-003 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, 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-H1:80

The web server on NET-B-H1:80 reports Apache version 2.4.29, which falls within the range affected by CVE-2021-41773 and CVE-2021-42013, path traversal vulnerabilities in Apache 2.4.x prior to 2.4.51. This was confirmed by Nessus, Nmap, and Nuclei.

IMPACT

Exploitation could allow an attacker to read arbitrary files or execute code on the server, potentially exposing sensitive data or leading to further compromise of the host.

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>
```

Template: CVE-2021-41773

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

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

VERIFICATION

To verify, re-run Nessus plugin 156032 against NET-B-H1, run: `nmap -p80 -sV --script vulners NET-B-H1`, and run: `nuclei -id CVE-2021-41773 -u http://NET-B-H1`

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade Apache HTTP Server to version 2.4.51 or later. Validate the update in a staging environment before production deployment. Restrict access to the web server pending patching if immediate upgrade is not possible.

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>

<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

Remediation roadmap

Immediate (priority 1)

Ce plan hiérarchise les actions correctives selon leur priorité de traitement. Les findings de priorité 1 regroupent des vulnérabilités critiques et des accès non authentifiés exposés (F-001 à F-013, F-017, F-018, F-022, F-023), incluant notamment des bases de données (MongoDB, Redis, PostgreSQL, MySQL) accessibles sans authentification, des identifiants par défaut (Tomcat), un fichier .env exposé, et plusieurs CVE critiques touchant des composants comme openssl, log4js et zlib. Ces éléments doivent être corrigés sans délai, en priorité les accès non authentifiés et les identifiants par défaut, qui constituent une exposition directe.

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
F-022 — Elasticsearch Unauthenticated Access
F-023 — Exposed .env file

Planned (priority 2)

Les findings de priorité 2 (F-014, F-015, F-016, F-019 à F-021, F-024 à F-028, F-034, F-037) sont classés en sévérité haute ou moyenne. Ils comprennent des CVE affectant des composants comme busybox, curl, glibc, openssl et lodash, ainsi que des faiblesses de configuration telles qu'un service Telnet non chiffré, un certificat SSL non fiable, et l'absence de NLA sur les services Terminal Services. Ces éléments doivent être intégrés au cycle de remédiation en cours, sans urgence immédiate mais sans report excessif.

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-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
F-034 — OpenSSH < 7.9 User Enumeration
F-037 — Terminal Services Doesn't Use NLA

Monitor (priority 3)

Les findings de priorité 3 (F-029 à F-036, F-038 à F-040) sont de sévérité moyenne ou faible. Ils incluent des CVE de sévérité moyenne sur des composants comme krb5, requests, ncurses, jinja2 et semver, ainsi que des observations liées aux algorithmes SSH faibles, aux suites de chiffrement SSL de force moyenne, et des observations générales de faible sévérité. Ces éléments ne nécessitent pas d'action immédiate mais doivent rester sous surveillance et être réévalués lors des prochains cycles d'audit.

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-035 — SSH Weak Algorithms Supported

F-036 — SSL Medium Strength Cipher Suites Supported

F-038 — Low-severity observations — information exposure

F-039 — Low-severity observations — TLS encryption

F-040 — 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-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

Technical annex

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

F-029	CVE-2022-42898 in krb5 1.18.3-6	MEDIUM	6.5	1
F-030	CVE-2023-32681 in requests 2.28.1	MEDIUM	6.1	1
F-031	CVE-2023-29491 in ncurses 6.2-1	MEDIUM	5.5	1
F-032	CVE-2024-22195 in jinja2 3.0.3	MEDIUM	5.4	1
F-033	CVE-2022-25883 in semver 7.3.5	MEDIUM	5.3	1
F-034	OpenSSH < 7.9 User Enumeration	MEDIUM	5.3	1
F-035	SSH Weak Algorithms Supported	MEDIUM	5.3	1
F-036	SSL Medium Strength Cipher Suites Supported	MEDIUM	5.3	2
F-037	Terminal Services Doesn't Use NLA	MEDIUM	5.3	1
F-038	Low-severity observations — information exposure	LOW		5
F-039	Low-severity observations — TLS encryption	LOW		5
F-040	Low-severity observations — web services	LOW		6

Annex — Re-test

To be completed during remediation verification.

REF	TITLE	STATUS	DATE	VERIFICATION
F-001	CVE-2021-44228 in log4js 6.3.0	Open		
F-002	vsftpd Smiley Face Backdoor	Open		
F-003	Apache 2.4.x < 2.4.51 Path Traversal	Open		
F-004	CVE-2021-3711 in openssl 1.1.1k	Open		
F-005	CVE-2022-3602 in openssl 3.0.5-1	Open		
F-006	CVE-2022-37434 in zlib 1.2.12-r1	Open		
F-007	Fortinet FortiOS Path Traversal	Open		
F-008	Jenkins unauthenticated dashboard	Open		
F-009	MongoDB Unauthenticated Access	Open		
F-010	MySQL Unpassworded Account Check	Open		
F-011	OpenSSL 3.0.0 < 3.0.7 Buffer Overflow	Open		
F-012	PostgreSQL Default Credentials	Open		
F-013	Redis Server Unprotected Access	Open		
F-014	CVE-2022-28391 in busybox 1.35.0-r17	Open		
F-015	CVE-2023-38545 in curl 7.83.1-r3	Open		
F-016	Jenkins < 2.235.2 Multiple Vulnerabilities	Open		
F-017	Tomcat manager default credentials	Open		
F-018	MS17-010 SMB Remote Code Execution	Open		
F-019	CVE-2023-4911 in glibc 2.31-13	Open		
F-020	CVE-2022-3786 in openssl 3.0.5-1	Open		
F-021	CVE-2022-4450 in openssl 1.1.1q-r0	Open		
F-022	Elasticsearch Unauthenticated Access	Open		
F-023	Exposed .env file	Open		
F-024	SMTP Service STARTTLS Plaintext Injection	Open		
F-025	SSL Certificate Cannot Be Trusted	Open		

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