

CABINET DÉMO

Container and dependency audit

Security assessment report

PREPARED BY Cabinet Démo

DATE 05/08/2026

SCOPE Application images

Executive dashboard

16 VULNERABILITIES	4 CRITICAL	7 HIGH
2 AFFECTED ASSETS	7.7 AVERAGE CVSS	2 REMOTE / UNAUTHENTICATED

90 /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 7 · MEDIUM 5
--	---

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, leading to data breach or service disruption. HOST-01
F-002 CVE-2021-3711 in openssl 1.1.1k
Exploitation could allow memory corruption leading to code execution or denial of service, affecting system availability and integrity. HOST-01
F-003 CVE-2022-3602 in openssl 3.0.5-1
Exploitation could result in memory corruption, potentially leading to service crash or code execution, impacting service continuity. HOST-01

Attack path

FOOTHOLD	F-001 CVE-2021-44228 in log4js 6.3.0 HOST-01 Unauthenticated
ESCALATION	F-002 CVE-2021-3711 in openssl 1.1.1k HOST-01 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 4 FINDINGS
Contain remote code execution and

unauthenticated access.

Owner: Infrastructure & DevOps · Effort: Medium
F-001, F-002, F-003, F-004

Phase 2 SHORT TERM · 8-30 DAYS 7 FINDINGS

Fix high-severity services and remove weak credentials.

Owner: Infrastructure & DevOps · Effort: Medium
F-005, F-006, F-007, F-008, F-009, F-010 ...

Phase 3 MEDIUM TERM · 31-90 DAYS 5 FINDINGS

Harden configuration, TLS and monitoring; retest the scope.

Owner: Infrastructure & DevOps · Effort: Medium
F-012, F-013, F-014, F-015, F-016

Document control

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

Executive summary

Cet audit a port  sur les composants logiciels utilis s par les services applicatifs de l'entreprise (API, worker et biblioth ques associ es). L'analyse identifie quatre failles critiques et huit failles de s v rit   lev e, principalement li es   des composants tiers obsol tes (biblioth ques de chiffrement, compression et traitement de donn es). Aucune de ces failles n'est actuellement recens e comme exploit e activement, mais leur s v rit  justifie une correction prioritaire. La direction doit d cider d'un calendrier de mise   jour des composants concern s et allouer les ressources techniques n cessaires pour r duire l'exposition avant qu'un incident ne survienne.

Top risks

- Une compromission des services applicatifs pourrait entra ner une interruption d'activit  et une perte de disponibilit  pour les utilisateurs.
- Une exploitation des failles li es au chiffrement pourrait exposer des donn es sensibles et engager la responsabilit  de l'entreprise en mati re de protection des donn es.
- Une ex cution de code non autoris e sur les services concern s pourrait permettre   un attaquant de prendre le contr le partiel de l'infrastructure, avec un risque de propagation   d'autres syst mes.

Severity distribution

SEVERITY	#	%	
CRITICAL	4	25%	
HIGH	7	44%	
MEDIUM	5	31%	
LOW	0	0%	
INFO	0	0%	

Scope and methodology

In scope

Application images

2 host(s)

HOST-01, HOST-02

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
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	CVE-2021-3711 in openssl 1.1.1k	CRITICAL	9.8	1	Open
F-003	CVE-2022-3602 in openssl 3.0.5-1	CRITICAL	9.8	1	Open
F-004	CVE-2022-37434 in zlib 1.2.12-r1	CRITICAL	9.8	1	Open
F-005	CVE-2022-28391 in busybox 1.35.0-r17	HIGH	8.8	2	Open
F-006	CVE-2023-38545 in curl 7.83.1-r3	HIGH	8.8	2	Open
F-007	CVE-2023-4911 in glibc 2.31-13	HIGH	7.8	2	Open
F-008	CVE-2022-3786 in openssl 3.0.5-1	HIGH	7.5	2	Open
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	HIGH	7.5	2	Open
F-010	CVE-2020-8203 in lodash 4.17.15	HIGH	7.4	2	Open
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	HIGH	7.4	2	Open
F-012	CVE-2022-42898 in krb5 1.18.3-6	MEDIUM	6.5	3	Open
F-013	CVE-2023-32681 in requests 2.28.1	MEDIUM	6.1	3	Open
F-014	CVE-2023-29491 in ncurses 6.2-1	MEDIUM	5.5	3	Open
F-015	CVE-2024-22195 in jinja2 3.0.3	MEDIUM	5.4	3	Open
F-016	CVE-2022-25883 in semver 7.3.5	MEDIUM	5.3	3	Open

Findings — detail

Extract: 3 of 16 findings are written up below. The remaining 13, 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 container image HOST-03/api:1.4.2 includes log4js 6.3.0, affected by CVE-2021-44228. A fixed version (6.4.0) is available. This vulnerability is classified as CWE-502.

IMPACT

Exploitation could allow an attacker to compromise the application, leading to data breach or service disruption.

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: trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Upgrade log4js to version 6.4.0 or later in the affected image. Rebuild and redeploy the api image. Verify the fix with a new image scan.

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 CVE-2021-3711 in openssl 1.1.1k

CRITICAL CVSS 9.8 CWE-787 CVE-2021-3711 Sources: TRIVY

Sévérité critical : score CVSS de 9.8.

AFFECTED ASSETS

HOST-01

The container image HOST-03/api:1.4.2 runs openssl 1.1.1k, affected by CVE-2021-3711 (CWE-787). A fixed version (1.1.1l) is available.

IMPACT

Exploitation could allow memory corruption leading to code execution or denial of service, affecting system availability and integrity.

EVIDENCE

```
Target: HOST-03/api:1.4.2 (debian 11.6)
Package: openssl
```

Installed version: 1.1.1k
Fixed version: 1.1.1l
Vulnerability: CVE-2021-3711

VERIFICATION

To verify: trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Update the openssl package to version 1.1.1l or later. Rebuild the base image and redeploy. Re-scan the image to confirm remediation.

REFERENCES

<https://nvd.nist.gov/vuln/detail/CVE-2021-3711>
<https://cwe.mitre.org/data/definitions/787.html>

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

F-003 CVE-2022-3602 in openssl 3.0.5-1

CRITICAL CVSS 9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-787 CVE-2022-3602 Sources: TRIVY

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

HOST-01

The container image HOST-03/api:1.4.2 uses openssl 3.0.5-1, affected by CVE-2022-3602 (CWE-787). A fixed version (3.0.7-1) is available.

IMPACT

Exploitation could result in memory corruption, potentially leading to service crash or code execution, impacting service continuity.

EVIDENCE

Target: HOST-03/api:1.4.2 (debian 11.6)
Package: openssl
Installed version: 3.0.5-1
Fixed version: 3.0.7-1
Vulnerability: CVE-2022-3602

VERIFICATION

To verify: trivy image --severity HIGH,CRITICAL HOST-03/api:1.4.2

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Update openssl to version 3.0.7-1 or later. Rebuild the image and redeploy. Confirm remediation via a fresh vulnerability scan.

REFERENCES

<https://nvd.nist.gov/vuln/detail/CVE-2022-3602>
<https://cwe.mitre.org/data/definitions/787.html>

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

Remediation roadmap

Immediate (priority 1)

This remediation plan is organized in three tiers based on the severity and priority assigned to each finding.

Four critical vulnerabilities require immediate treatment: F-001 (CVE-2021-44228 in log4js 6.3.0), F-002 (CVE-2021-3711 in openssl 1.1.1k), F-003 (CVE-2022-3602 in openssl 3.0.5-1), and F-004 (CVE-2022-37434 in zlib 1.2.12-r1). None are flagged as known exploited (KEV) in the data provided, but their critical severity justifies prompt patching. Affected components should be updated to non-vulnerable versions as a priority action.

F-001 — CVE-2021-44228 in log4js 6.3.0

F-002 — CVE-2021-3711 in openssl 1.1.1k

F-003 — CVE-2022-3602 in openssl 3.0.5-1

F-004 — CVE-2022-37434 in zlib 1.2.12-r1

Planned (priority 2)

Seven high-severity findings should be addressed within the current remediation cycle: F-005 (busybox), F-006 (curl), F-007 (glibc), F-008 and F-009 (openssl), F-010 (lodash), and F-011 (openssl). These are not flagged as KEV in the data provided. They should be scheduled for patching alongside regular maintenance windows, in line with internal change management processes.

F-005 — CVE-2022-28391 in busybox 1.35.0-r17

F-006 — CVE-2023-38545 in curl 7.83.1-r3

F-007 — CVE-2023-4911 in glibc 2.31-13

F-008 — CVE-2022-3786 in openssl 3.0.5-1

F-009 — CVE-2022-4450 in openssl 1.1.1q-r0

F-010 — CVE-2020-8203 in lodash 4.17.15

F-011 — CVE-2023-0286 in openssl 1.1.1q-r0

Monitor (priority 3)

Five medium-severity findings fall into this category: F-012 (krb5), F-013 (requests), F-014 (ncurses), F-015 (jinja2), and F-016 (semver). None are flagged as known exploited. No immediate action is required, but these items should remain tracked and reassessed in future scans to confirm their status does not evolve.

F-012 — CVE-2022-42898 in krb5 1.18.3-6

F-013 — CVE-2023-32681 in requests 2.28.1

F-014 — CVE-2023-29491 in ncurses 6.2-1

F-015 — CVE-2024-22195 in jinja2 3.0.3

F-016 — CVE-2022-25883 in semver 7.3.5

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.8.8	Management of technical vulnerabilities	F-001, F-002, F-003, F-004, F-005, F-006, F-007, F-008, F-009, F-010, F-011, F-012, F-013, F-014, F-015, F-016

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-010, F-011, F-012, F-013, F-014, F-015, F-016

Technical annex

REF	TITLE	SEVERITY	CVSS	ASSETS
F-001	CVE-2021-44228 in log4js 6.3.0	CRITICAL	10.0	1
F-002	CVE-2021-3711 in openssl 1.1.1k	CRITICAL	9.8	1
F-003	CVE-2022-3602 in openssl 3.0.5-1	CRITICAL	9.8	1
F-004	CVE-2022-37434 in zlib 1.2.12-r1	CRITICAL	9.8	1
F-005	CVE-2022-28391 in busybox 1.35.0-r17	HIGH	8.8	1
F-006	CVE-2023-38545 in curl 7.83.1-r3	HIGH	8.8	2
F-007	CVE-2023-4911 in glibc 2.31-13	HIGH	7.8	1
F-008	CVE-2022-3786 in openssl 3.0.5-1	HIGH	7.5	1
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	HIGH	7.5	1
F-010	CVE-2020-8203 in lodash 4.17.15	HIGH	7.4	1
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	HIGH	7.4	1
F-012	CVE-2022-42898 in krb5 1.18.3-6	MEDIUM	6.5	1
F-013	CVE-2023-32681 in requests 2.28.1	MEDIUM	6.1	1
F-014	CVE-2023-29491 in ncurses 6.2-1	MEDIUM	5.5	1
F-015	CVE-2024-22195 in jinja2 3.0.3	MEDIUM	5.4	1
F-016	CVE-2022-25883 in semver 7.3.5	MEDIUM	5.3	1

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	CVE-2021-3711 in openssl 1.1.1k	Open		
F-003	CVE-2022-3602 in openssl 3.0.5-1	Open		
F-004	CVE-2022-37434 in zlib 1.2.12-r1	Open		
F-005	CVE-2022-28391 in busybox 1.35.0-r17	Open		
F-006	CVE-2023-38545 in curl 7.83.1-r3	Open		
F-007	CVE-2023-4911 in glibc 2.31-13	Open		
F-008	CVE-2022-3786 in openssl 3.0.5-1	Open		
F-009	CVE-2022-4450 in openssl 1.1.1q-r0	Open		
F-010	CVE-2020-8203 in lodash 4.17.15	Open		
F-011	CVE-2023-0286 in openssl 1.1.1q-r0	Open		
F-012	CVE-2022-42898 in krb5 1.18.3-6	Open		
F-013	CVE-2023-32681 in requests 2.28.1	Open		
F-014	CVE-2023-29491 in ncurses 6.2-1	Open		
F-015	CVE-2024-22195 in jinja2 3.0.3	Open		
F-016	CVE-2022-25883 in semver 7.3.5	Open		