ZERO | TOLERANCE

FINAL

COORDINATED DISCLOSURE ADVISORY - ZT-2026-VU487875-ADV

Multiple Vulnerabilities - Deloitte AI Assist (Ascend Platform)

CVE-2026-TBD-001 THROUGH CVE-2026-TBD-005

Five classes of high-severity vulnerabilities affecting six tenant deployments of the Deloitte AI Assist (Ascend) platform. Findings include unauthenticated Keycloak admin consoles, twelve backend API endpoints exposed without authentication, SSRF via configuration injection, password-grant authentication on public OAuth clients, and unauthenticated RAG corpus access with confirmed write-path. Coordinated through CERT/CC VU#487875 + CISA VRC. Public disclosure 2026-05-18.

DATE
18 May 2026

SUBJECT
Deloitte AI Assist (Ascend Platform)

PREPARED BY
Zero|Tolerance Security Research (zerotolerance.me)

CLASSIFICATION
PUBLIC DISCLOSURE - zerotolerance.me + CERT/CC public Vulnerability Note

Multiple Vulnerabilities in Deloitte AI Assist (Ascend Platform)

Coordinated Disclosure Advisory

Field	Value
Advisory ID	ZT-2026-VU487875-ADV
Case ID	CERT/CC VU#487875
Vendor	Deloitte Touche Tohmatsu Limited
Product	Deloitte AI Assist (Ascend Platform)
Affected Components	Identity (Keycloak), API gateway (Azure APIM), backend services (auth-service, app-config, rag-service), client-side configuration bundle
CVE Identifiers	CVE-2026-TBD-001 through CVE-2026-TBD-005 (coordinated through CERT/CC)
CWE Categories	CWE-306, CWE-918, CWE-521, CWE-200, CWE-639
CVSS v3.1 (highest)	9.1 CRITICAL
Initial Disclosure	2026-03-13 (Deloitte Canada CISO, direct)
CERT/CC Case Opened	2026-04-17
CISA VRC Coordination	2026-04-21 (eoinWM, ANALYGENCE / CISA Vulnerability Response Coordination)
Vendor Engagement on Coordination Thread	2026-05-08
Public Disclosure	2026-05-18
Researcher	Karim El Labban, Zero|Tolerance Security Research

1. Executive Summary

Zero|Tolerance Security Research identified five classes of high-severity vulnerabilities in Deloitte's AI Assist platform (internally branded Ascend), an enterprise AI/ML workflow product delivered as multi-tenant SaaS to Fortune 500 clients. The vulnerabilities were observed in every assessed tenant deployment (6 of 6), including Deloitte's own production and development environments.

Findings include unauthenticated access to Keycloak administrative consoles across six production tenants, twelve backend API endpoints exposed without authentication on the primary assessment subject, server-side request forgery via configuration injection, password-grant authentication exposed on public OAuth clients with no rate limiting, and unauthenticated access to retrieval-augmented generation (RAG) document corpora with confirmed write-path for content poisoning.

All findings are exploitable from the public internet using only standard HTTP requests. No credentials, no authentication bypass, no exploitation primitives are required. The vulnerabilities were verified via passive reconnaissance and read-only API interaction. Reassessment activity across Day 3/4 (2026-03-19), Day 8 (2026-03-24), and Day 63 (2026-05-16) records a divergent remediation posture by environment: substantial decommission and rebuild work at five of six client environments, an active regression at the production Keycloak layer, and one architectural defect (password grant on public OAuth clients) that remains unfixed at Day 63. See Section 5 for the per-bucket Day 63 disposition.

Risk Evaluation

Dimension	Assessment
Attack Vector	Network (public internet)
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed (cross-tenant impact via SSRF + shared identity infrastructure)
Confidentiality	High (client document corpora, identity tokens, configuration data)
Integrity	High (RAG corpus write-path, configuration injection)
Availability	High (production identity infrastructure, brute-force vector)
CVSS v3.1 (highest)	9.1 CRITICAL
Exploitation Status	No known in-the-wild exploitation observed by Zero|Tolerance Security Research

2. Affected Products

Deloitte AI Assist platform (Ascend), deployed across the following observed tenants. Each tenant operates as an independent multi-tenant slice of the shared platform infrastructure:

Tenant	Deployment Type	Industry Sector	Status
Primary assessment subject	Client production	Medical device manufacturing	Unauthenticated access verified
Additional Fortune 500 tenant A	Client production	Healthcare device	Cross-tenant API access verified
Additional Fortune 500 tenant B	Client production	Automotive aftermarket	Cross-tenant API access verified
Additional Fortune 500 tenant C	Client production	Sleep medicine	Cross-tenant API access verified
Deloitte Production	Internal	N/A	Unauthenticated access verified
Deloitte Dev/QA/PreProd	Internal	N/A	Unauthenticated access verified

Each tenant operates a dedicated Keycloak identity instance, Azure API Management gateway, and backend service mesh, all internet-exposed.

> **Note:** Tenant identities for A, B, and C are documented in CERT/CC VINCE case materials and available to the coordinator for vendor notification. This advisory presents corroborating tenant evidence in sector form to demonstrate the tenant-model defect without expanding incident disclosure beyond the primary assessment scope. Notification of affected tenants is a vendor responsibility under coordinated vulnerability disclosure norms.

---

3. Vulnerability Overview

3.1 CVE-2026-TBD-001 - Unauthenticated Keycloak Administrative Console Exposure

Field	Value
CWE	CWE-306 Missing Authentication for Critical Function
CVSS v3.1	7.5 HIGH (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Affected Component	Keycloak instances backing each AI Assist tenant
Instances Confirmed	6 (one per tenant)

Description. Six Keycloak administrative consoles backing the AI Assist platform return HTTP 200 to unauthenticated requests on the public internet. Each console serves a distinct production tenant and exposes identical resource hashes across the population, indicating a shared deployment template that propagates the misconfiguration to every new tenant onboarded to the platform.

Impact. An unauthenticated remote attacker can enumerate realm configurations, observe OIDC client identifiers, and identify the full grant-type catalog supported by each realm. Combined with finding 3.4 (password grant), this provides the prerequisites for credential brute-force against the production identity plane.

Evidence. All six consoles return HTTP 200 with response body sizes between 3,380 and 4,018 bytes. Resource version hashes are identical across original disclosure (2026-03-13) and reassessment (2026-03-24), confirming zero patch deployment.

3.2 CVE-2026-TBD-002 - Unauthenticated Backend API Endpoints

Field	Value
CWE	CWE-306 Missing Authentication for Critical Function
CVSS v3.1	9.1 CRITICAL (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
Affected Component	Backend services (auth-service, app-config, rag-service) behind Azure APIM
Endpoints Confirmed	12 on primary tenant; cross-tenant access verified on 4 additional tenant gateways

Description. Twelve backend API endpoints across three services accept unauthenticated requests via the public Azure API Management gateway. The same endpoint pattern returns identical unauthenticated responses on the API Management gateways of all four additional tenants, confirming the deficiency is shared across the tenant population rather than localized to the primary assessment subject.

Endpoint inventory (primary tenant):

#	Endpoint	Method	Behavior Without Auth
1	`/auth-service/v1/manage/user/token/fetch`	POST	User enumeration via differential 400 response
2	`/auth-service/v1/manage/user/token`	POST	Parameter disclosure via 400 validation error
3	`/app-config/v1/config/get-instance`	GET	Returns full configuration with internal URLs
4	`/app-config/v1/config/project`	GET	Returns project array
5	`/rag-service/v1/rag/retrieval`	POST	RAG corpus query without auth
6	`/rag-service/v1/rag/file-content-retrieval`	POST	File content retrieval from RAG corpus
7	`/rag-service/v1/rag/general-content-file-ingestion`	POST	RAG corpus write-path (see 3.5)
8-12	Additional `/auth-service/v1/manage/*` endpoints	Various	Various unauthenticated behaviors

Authentication control verified. The corresponding v2 endpoint (`/auth-service/v2/manage/user/all`) correctly returns HTTP 401 "Missing Authorization header" to identical unauthenticated requests, confirming the v1 endpoints lack authentication by configuration deficiency, not platform-wide auth absence.

Cross-tenant verification. The token-fetch endpoint returns the equivalent user-enumeration response on the API Management gateways of all four additional tenants. Each gateway processes unauthenticated requests against its respective backend.

3.3 CVE-2026-TBD-003 - Server-Side Request Forgery via Configuration Injection

Field	Value
CWE	CWE-918 Server-Side Request Forgery
CVSS v3.1	8.1 HIGH (AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L)
Affected Component	`/app-config/v1/config/get-instance` write-path
Confirmation	Two records with corroborated HTTP capture (id:9, id:10); two further records (id:11, id:12) described in technical-delivery drafts without contemporaneous capture; all four occupy the id:9 through id:12 range

Description. The configuration write-path accepts unauthenticated POST requests that persist arbitrary `base_url` values into the production configuration store. The `base_url` field is consumed by downstream RAG and integration services that issue server-side HTTP requests to the configured URL.

Confirmation. During the original assessment (2026-03-13), Zero\|Tolerance Security Research wrote between two and four test records to the production configuration store via the unauthenticated `/app-config/v1/config/get-instance` endpoint to verify the SSRF primitive, occupying IDs in the range id:9 through id:12. The two records with the strongest evidentiary support are id:9 (empty string `base_url`) and id:10 (`base_url` set to `https://deloitte.atlassian.net`), both corroborated by reassessment passes on 2026-03-19 and 2026-03-24. Two further records (id:11 with `base_url` set to a tenant-controlled Jira hostname, FQDN redacted and available to coordinator; id:12 with `base_url` set to a tenant-controlled Atlassian Cloud hostname, FQDN redacted and available to coordinator) are described in technical-delivery drafts of this finding but lack contemporaneous HTTP capture; they are reported here in the interest of full disclosure with the asymmetry of evidence noted. All record values reference either an empty string or a vendor-controlled or tenant-controlled Atlassian Cloud URL; no record points to attacker-controlled infrastructure. All records remained present in the production configuration store at the Day 8 reassessment, eleven days after vendor notification. The persistence of these test records supports the following observations:

1. The configuration write-path lacks authentication
2. The configuration store had not been audited for unauthorized records as of the reassessment date

Impact. An unauthenticated remote attacker can redirect downstream service-to-service requests to attacker-controlled infrastructure, capture authentication tokens issued by the platform to integration partners (Atlassian Jira, observed in the injected test configuration), and pivot to internal-only services reachable from the backend service mesh.

3.4 CVE-2026-TBD-004 - Password Grant Enabled on Public OAuth Clients Without Rate Limiting

Field	Value
CWE	CWE-521 Weak Password Requirements (operational, paired with CWE-307 missing brute-force protection)
CVSS v3.1	8.1 HIGH (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
Affected Component	Keycloak OIDC clients (`web-app-client`, `admin-cli`) across multiple realms
Instances Confirmed	6+ realms (one per tenant plus master realms)

Description. The OIDC configuration for the AI Assist platform exposes seven grant types on the public OAuth client, including `password` (Resource Owner Password Credentials) and `implicit`. The `admin-cli` client is active on the master realm of multiple instances. Password-grant requests against `web-app-client` and `admin-cli` produce `"Invalid user credentials"` responses, confirming the grant type is processed by the identity plane. No rate-limiting was observed on the public endpoint.

Full `grant_types_supported` (as of 2026-03-19):

```
[
  "authorization_code",
  "implicit",
  "refresh_token",
  "password",
  "client_credentials",
  "urn:openid:params:grant-type:ciba",
  "urn:ietf:params:oauth:grant-type:device_code"
]
```

Impact. Combined with finding 3.2 (user enumeration via token-fetch), an unauthenticated remote attacker can enumerate valid usernames against the production identity plane and then brute-force credentials against those accounts without rate limiting. Successful credential capture yields full identity-plane access including the administrative API surface accessible to `admin-cli`.

3.5 CVE-2026-TBD-005 - Unauthenticated RAG Corpus Access and Content Poisoning

Field	Value
CWE	CWE-639 Authorization Bypass Through User-Controlled Key
CVSS v3.1	9.1 CRITICAL (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
Affected Component	`rag-service` endpoints (retrieval + file-content-retrieval + general-content-file-ingestion)
Confirmation	Three RAG endpoints respond to unauthenticated POST requests

Description. Three retrieval-augmented generation (RAG) endpoints accept unauthenticated requests against the production RAG corpus. The `retrieval` and `file-content-retrieval` endpoints expose stored document content; the `general-content-file-ingestion` endpoint provides a write-path into the corpus.

The RAG corpus contains client documents indexed for use by the AI Assist workflow. Unauthenticated read access permits exfiltration of client intellectual property, internal documents, and personally identifiable information that has been ingested by client end-users. Unauthenticated write access permits injection of attacker-controlled content into the corpus. The write-path was demonstrated to accept unauthenticated POST requests; round-trip surfacing through the AI Assist retrieval pipeline was not tested per scope discipline.

Impact. Two distinct attacker primitives:

1. **Exfiltration.** An unauthenticated remote attacker can query and retrieve any document indexed in the production RAG corpus across affected tenants.
2. **Poisoning.** An unauthenticated remote attacker can ingest arbitrary content into the production RAG corpus, which is then returned to authorized end-users as authoritative reference material via the platform's AI-generated outputs.

---

4. Coordination Timeline

Date	Event
2026-03-12 to 2026-03-13	Initial assessment of Deloitte internet-facing infrastructure (passive reconnaissance)
2026-03-13	Direct disclosure to Deloitte Canada Chief Information Security Officer
2026-03-19	Day 3/4 post-disclosure reassessment: zero remediation observed
2026-03-20	Day 7 observation: six Keycloak administrative consoles return HTTP 404 to public requests (network-layer restriction applied)

Date	Event
2026-03-24	Day 8 post-disclosure reassessment: five APIM gateways unreachable / firewalled at network layer; six Keycloak admin consoles confirmed 404; ~46 items moved to "not externally verifiable" state
2026-04-17	CERT/CC case opened (VU#487875)
2026-04-21	CISA Vulnerability Response Coordination engaged; case migrated to CISA VRC
2026-04-29	Reassessment supplements uploaded to VINCE Documents
2026-05-08	Vendor (Deloitte Ascend Platform) engaged on case coordination thread
2026-05-12	Publication anchor proposed at 2026-05-18 via coordination thread
2026-05-16	Day 63 post-disclosure reassessment: divergent remediation posture recorded (see Section 5)
2026-05-18	Public disclosure (this advisory)

---

5. Remediation Status

Reassessments were conducted at Day 3/4 (2026-03-19), Day 8 (2026-03-24), and Day 63 (2026-05-16) post-disclosure, each applying the same passive-reconnaissance methodology used in the original assessment.

Between Day 8 and Day 63 the remediation picture diverged sharply by environment. The disposition below replaces the Day 8 "no remediation observed" picture with the Day 63 per-bucket assessment.

5.1 Remediated and Externally Verified at Day 63

The following items are remediated to a stronger state than the Day 8 perimeter posture and the remediation is independently verifiable from the public internet:

Item	Day 8 Status	Day 63 Status
Keycloak admin console - Primary tenant (codename `yellowmeadow`)	HTTP 404	NXDOMAIN; container app decommissioned; client frontend now redirects to a replacement Keycloak instance on Azure Private Link (codename `kindrock`, not publicly reachable)
Keycloak admin console - Tenant A (codename `icysmoke`)	HTTP 404	NXDOMAIN; container app decommissioned
Keycloak admin console - Tenant B (codename `redcoast`)	HTTP 404	NXDOMAIN; container app decommissioned; client frontend now redirects to a replacement Keycloak instance on Azure Private Link (codename `agreeablesea`, not publicly reachable)

Item	Day 8 Status	Day 63 Status
Keycloak admin console - Tenant C (codename `kindfield`)	HTTP 404	NXDOMAIN; container app decommissioned
Keycloak admin console - Dev/QA/PreProd (codename `blacksky`)	HTTP 404	NXDOMAIN; container app decommissioned
APIM gateway - Primary tenant	Firewalled / unreachable	NXDOMAIN; gateway removed
APIM gateway - Tenant A	Firewalled / unreachable	NXDOMAIN; gateway removed
APIM gateway - Tenant B	Firewalled / unreachable	NXDOMAIN; gateway removed
APIM gateway - Tenant C	Firewalled / unreachable	NXDOMAIN; gateway removed
APIM vanity CNAME (`apim.aiassist.deloitte.com`)	Firewalled / unreachable	NXDOMAIN
Endpoint `/app-config/v1/config/project` on Production APIM	HTTP 200 unauthenticated (returned project array)	HTTP 401; authentication now enforced at the application layer (see Section 5.1.a)
Client-side configuration bundles on the two reachable client frontends	Five bundles still served as of Day 8	All three known bundle paths (`/assets/index-Bg23105H.js`, `/assets/index-CP3GY4O1.js`, `/assets/index-l7TJwn3V.js`) return HTTP 404 on the reachable frontends

Section 5.1.a Application-layer fix confirmation. Day 8 noted that application-layer remediation was not externally verifiable post-firewall, since gateway firewalling closes the external observation surface without confirming the underlying authentication state of the services behind the gateway. The Day 63 reassessment found one endpoint where the application-layer state is now externally observable: `/app-config/v1/config/project` on the production APIM (now retopologized to a tenant-controlled Azure App Service hostname, FQDN redacted and available to coordinator) returns HTTP 401 to anonymous requests where Day 0 returned HTTP 200 with an unauthenticated project array. This is the first externally-observable evidence of genuine application-layer authentication enforcement on a previously-unauthenticated endpoint of the platform.

5.2 Not Externally Verifiable Post-Fix

Approximately 45 items moved into a state where the internal application-layer remediation status cannot be assessed from external reconnaissance. The infrastructure rebuilds at the two client environments rebuilt on Azure Private Link (the `kindrock` and `agreeablesea` replacement Keycloak instances and the corresponding application backend) are not publicly reachable, so the OIDC grant-type configuration, the `admin-cli` master-realm posture, the unauthenticated endpoint inventory, and the identity-token-theft vector status cannot be probed externally on those environments. The same applies to the three other client environments where the gateway infrastructure was decommissioned outright at the DNS layer.

The state of these items at Day 63 is consistent with a remediation pattern in which the underlying defects may have been addressed, may have been carried into the rebuilt infrastructure, or may have been mooted by the decommission. External reassessment methodology cannot distinguish among these states.

Persistence and cleanup status of the V3 test records (id:9 through id:12) is similarly opaque at Day 63: the `/app-config/v1/config/get-instance` endpoint that previously exposed the records returns HTTP 404 on the retopologized production APIM, and the four other APIM gateways are NXDOMAIN.

5.3 Regressed Since Day 8

One item observed at Day 8 in a remediated state is, at Day 63, no longer remediated:

Production Keycloak administrative console (`ai-assist2prd-keycloak-contapp1.redforest-4919d15e.eastus.azurecontainerapps.io`)

Field	Day 8 (2026-03-24)	Day 63 (2026-05-16)
`/admin/master/console/` response	HTTP 404	HTTP 200, full Keycloak Administration Console
Resource version identifier in served HTML	(not served)	`8yof5`
OIDC discovery on `master` realm	(not observable)	HTTP 200, full discovery document
OIDC discovery on `ai-assist-prod` realm	(not observable)	HTTP 200, full discovery document

The resource version identifier `8yof5` served at Day 63 matches the identifier captured in the original 2026-03-13 recon for this instance (recorded in Section A.8 of this advisory). The instance is in the same configuration state as Day 0. The Day 8 network-layer state that returned HTTP 404 to public requests is no longer present at Day 63; the instance returns HTTP 200 on the same path.

The `grant_types_supported` payload returned by the `ai-assist-prod` realm OIDC discovery at Day 63 is:

```
[
  "authorization_code",
  "implicit",
  "refresh_token",
  "password",
  "client_credentials",
  "urn:openid:params:grant-type:ciba",
  "urn:ietf:params:oauth:grant-type:device_code"
]
```

This payload is identical to the `grant_types_supported` captured at the original 2026-03-19 OIDC enumeration (see Section 3.4 of this advisory). The `password` grant type underlying finding 3.4 remains enabled on the production Keycloak.

5.4 Never Remediated

One finding is unchanged between Day 0 and Day 63 at the production Keycloak:

Finding 3.4 - Password Grant on Public OAuth Clients. The architectural design choice to expose the OAuth Resource Owner Password Credentials grant type on the public `web-app-client`, paired with the `implicit` grant type and the absence of observed rate limiting on the public endpoint, is present at the production Keycloak at both Day 0 and Day 63, with no public-internet-boundary fix applied at any point in the reassessment cycle. This bucket is distinct from Section 5.3: Section 5.3 records an item whose Day 8 state differed from Day 63 state; Section 5.4 records an item whose Day 0, Day 8, and Day 63 states are equivalent.

5.5 Remediation Scorecard at Day 63

Category	Tracked Items	Section 5.1 Remediated & Verified	Section 5.2 Not Externally Verifiable	Section 5.3 Regressed	Section 5.4 Never Remediated
Keycloak administrative console exposure	6 instances	5	0	1 (Production)	0
Password grant on public OAuth client	6+ realms	0	5+ (behind decommission / Private Link)	0	1 (Production realm)
Master realm `admin-cli` active	3 instances	0	2	0	1 (Production master, observable via Section 5.3 OIDC)
Unauthenticated backend API endpoints	12 endpoints	12 (11 returning 404 post-decommission/ retopology; 1 returning HTTP 401 with auth enforcement per Section 5.1.a)	0	0	0
User enumeration via gateway	5 gateways	5 (4 NXDOMAIN + 1 retopologized App Service returning 404 on the user-enumeration path)	0	0	0
Identity token theft vectors	3 endpoints	3 (404 on retopologized prod APIM + decommissioned client APIMs)	0	0	0
Configuration injection / SSRF	1 endpoint	1 (external write-path closed via APIM retopology)	0	0	0
RAG document access and poisoning	3 endpoints	3 (404 on retopologized prod APIM + decommissioned client APIMs)	0	0	0
Keycloak version patching	6 instances	5 (decommissioned or rebuilt)	0	1 (Production, hash `8yof5` unchanged)	0

Category	Tracked Items	Section 5.1 Remediated & Verified	Section 5.2 Not Externally Verifiable	Section 5.3 Regressed	Section 5.4 Never Remediated
Client-side configuration bundle exposure	5 frontends	3 (404 on reachable frontends)	2 (frontends DNS-resolve but TCP-filtered)	0	0
Container identity disclosure	5 instances	5 (no longer externally observable post-decommission)	0	0	0
Injected test record cleanup	id:9-id:12	0	4 records (database state opaque from outside)	0	0
TOTAL	**59 items**	**42**	**13**	**2**	**2**

The Section 5.3 and Section 5.4 columns are intentionally distinguished: a reverted operational remediation (Section 5.3) and an unremediated architectural design choice (Section 5.4) carry different policy implications and require different remediation paths.

---

6. Mitigations

The following mitigations apply to the vendor and to any organization operating a multi-tenant identity-fronted SaaS platform with comparable architecture.

6.1 Immediate (within 24 hours of advisory publication)

- Restrict Keycloak administrative console access to authenticated administrative networks only. Block public-internet access at the load balancer or Azure Application Gateway layer.
- Disable the `password` grant type across all public-facing OAuth clients. Disable `implicit` grant.
- Disable `admin-cli` access on master realms. If `admin-cli` is required operationally, restrict to internal-only network reachability.
- Enforce authentication on all `/auth-service/v1/manage/*`, `/app-config/v1/config/*`, and `/rag-service/v1/rag/*` endpoints at the API Management gateway layer.
- Audit Keycloak realm exports for unauthorized OIDC clients added during the exposure window.

6.2 Within 7 days

- Audit the production configuration store for unauthorized records, including specifically the test records in the id:9 through id:12 range referenced in finding 3.3.

- Implement rate-limiting and account-lockout policies on the identity plane.
- Audit the RAG corpus for unauthorized ingested content.

6.3 Within 30 days

- Reassess the multi-tenant deployment template that propagates these defects across new tenant onboarding.
- Implement authentication-by-default policy for all internal service-to-service communication.
- Conduct third-party verification of remediation against the 59-item tracked inventory, with particular attention to Section 5.3 (regressed production Keycloak) and Section 5.4 (architectural password-grant defect).

6.4 Detection Guidance

- API Management gateway logs: review for unauthenticated 2xx responses on the endpoint patterns listed in Section 3.2 (`/auth-service/v1/manage/*`, `/app-config/v1/config/*`, `/rag-service/v1/rag/*`).
- Keycloak administrative console access logs: review for sessions originating from non-administrative networks during the exposure window.
- Configuration store audit: query for `base_url` values not matching the operator's allowlist of permitted integration partners.
- RAG corpus audit: review ingested documents for content lacking expected client-origin metadata during the exposure window.

6.5 CVSS Environmental Scoring

Operators should compute environmental CVSS using their own Confidentiality, Integrity, and Availability Requirement metrics. The base scores in Section 3 assume a high-value tenant; operators with lower data-sensitivity profiles may compute lower environmental scores, while operators with regulated-data tenants (healthcare, financial, government) may compute higher scores.

---

7. References

- CERT/CC VU#487875: https://kb.cert.org/vuls/id/487875
- CWE-306 Missing Authentication for Critical Function: https://cwe.mitre.org/data/definitions/306.html
- CWE-918 Server-Side Request Forgery: https://cwe.mitre.org/data/definitions/918.html
- CWE-521 Weak Password Requirements: https://cwe.mitre.org/data/definitions/521.html
- CWE-200 Information Exposure: https://cwe.mitre.org/data/definitions/200.html
- CWE-639 Authorization Bypass Through User-Controlled Key: https://cwe.mitre.org/data/definitions/639.html

- CVE assignments coordinated through CERT/CC at publication; identifiers will be appended upon issuance.

8. Acknowledgements

Coordinated through CERT/CC VINCE (VU#487875). CISA Vulnerability Response Coordination engaged as of 2026-04-21 (ANALYGENCE / CISA VRC).

This advisory was prepared by Karim El Labban, Zero|Tolerance Security Research. The findings were validated via passive reconnaissance and read-only API interaction. No credentials were used, created, or brute-forced. No data was exfiltrated beyond what was returned in standard HTTP responses to unauthenticated requests. All testing was conducted from a single attribution-clean IP. Test artifacts are documented in CERT/CC case materials.

Appendix A - Detailed Findings Annex

The following annex enumerates the full 59-item findings inventory tracked across the reassessment cycle. The annex is provided to support CVE-assignment review by the coordinating CNA and to provide the full assessment inventory supporting the five CVE classes presented in Section 3.

A.1 Keycloak Administrative Console Exposure (6 items)

#	Instance	Original Status	Day 3/4 (03-19)	Day 8 (03-24)
1	Primary tenant Keycloak	HTTP 200 unauth	HTTP 200 unauth (3,994 bytes, hash unchanged)	HTTP 200 unauth
2	Production Keycloak	HTTP 200 unauth	HTTP 200 unauth (4,018 bytes, hash unchanged)	HTTP 200 unauth
3	Tenant A Keycloak	HTTP 200 unauth	HTTP 200 unauth (3,962 bytes, hash unchanged)	HTTP 200 unauth
4	Tenant B Keycloak	HTTP 200 unauth	HTTP 200 unauth (3,958 bytes, hash unchanged)	HTTP 200 unauth
5	Tenant C Keycloak	HTTP 200 unauth	HTTP 200 unauth (3,966 bytes, hash unchanged)	HTTP 200 unauth
6	Dev/QA/PreProd Keycloak	HTTP 200 unauth	HTTP 200 unauth (3,380 bytes, hash unchanged)	HTTP 200 unauth

A.2 Password Grant and Master Realm `admin-cli` Active (10 items)

#	Item	Status at Day 8
7	`password` grant enabled on `web-app-client`	Active
8	`password` grant accepted by primary tenant realm	Active
9	`password` grant accepted by Tenant A realm	Active
10	`password` grant accepted by Tenant B realm	Active
11	`password` grant accepted by Tenant C realm	Active
12	`password` grant accepted by Production realm	Active
13	`admin-cli` accepts credentials on primary master realm	Active
14	`admin-cli` accepts credentials on Production master realm	Active
15	`admin-cli` accepts credentials on Dev master realm	Active
16	`implicit` grant type exposed via OIDC discovery	Active

A.3 Unauthenticated Backend API Endpoints - Primary Tenant (12 items)

#	Endpoint	Behavior
17	`/auth-service/v1/manage/user/token/fetch`	400 with user enumeration via email-not-found message
18	`/auth-service/v1/manage/user/token`	400 parameter disclosure
19-21	Additional `/auth-service/v1/manage/*` endpoints	Unauth response patterns consistent with finding class
22	`/app-config/v1/config/get-instance`	200 returns configuration with internal URLs
23	`/app-config/v1/config/project`	200 returns project array
24-25	Additional `/app-config/v1/config/*` endpoints	Unauth response patterns consistent with finding class
26	`/rag-service/v1/rag/retrieval`	400 validation error, no auth challenge
27	`/rag-service/v1/rag/file-content-retrieval`	400 validation error, no auth challenge
28	`/rag-service/v1/rag/general-content-file-ingestion`	400 validation error, no auth challenge; write-path

A.4 Cross-Tenant Unauthenticated Gateway Access (4 items)

#	Tenant Gateway	Response
29	Tenant A APIM	User enumeration on token-fetch endpoint
30	Tenant B APIM	User enumeration on token-fetch endpoint
31	Tenant C APIM	User enumeration on token-fetch endpoint
32	Production APIM	User enumeration on token-fetch endpoint

A.5 Identity Token Theft Vectors (3 items)

#	Endpoint	Vector
33	`/auth-service/v1/manage/user/token/fetch`	Returns stored integration tokens for identified users
34	`/auth-service/v1/manage/user/token`	Token storage write-path
35	`/auth-service/v1/manage/user/token/exchange`	Token exchange without auth

A.6 Configuration Injection / SSRF (1 item)

#	Endpoint	Status
36	`/app-config/v1/config/get-instance` POST	Write-path persists arbitrary `base_url` values; two records with corroborated HTTP capture (id:9, id:10) and two further records (id:11, id:12) described in technical-delivery drafts without contemporaneous capture, all four occupying the id:9 through id:12 range; external visibility into configuration store closed at Day 63 via APIM retopology

A.7 RAG Document Access and Poisoning (3 items)

#	Endpoint	Vector
37	`/rag-service/v1/rag/retrieval`	Unauth corpus query
38	`/rag-service/v1/rag/file-content-retrieval`	Unauth document content retrieval
39	`/rag-service/v1/rag/general-content-file-ingestion`	Unauth corpus write (poisoning primitive)

A.8 Keycloak Version Patching (6 items)

#	Instance	Resource Hash (Day 8)	Patch Status
40	Primary tenant Keycloak	`ke8ae`	Unpatched since original assessment
41	Production Keycloak	`8yof5`	Unpatched since original assessment
42	Tenant A Keycloak	`mpk9w`	Unpatched since original assessment
43	Tenant B Keycloak	`b9dy5`	Unpatched since original assessment
44	Tenant C Keycloak	`lbdwd`	Unpatched since original assessment
45	Dev/QA/PreProd Keycloak	`lhquu`	Unpatched since original assessment

A.9 Client-Side Configuration Bundle Exposure (5 items)

#	Frontend	Bundle Status
46	Primary tenant frontend (`index-l7TJwn3V.js`)	Bundle hash identical to original disclosure date
47	Production frontend	Bundle 759 bytes, unchanged
48	Tenant A frontend	Bundle 759 bytes, unchanged
49	Tenant B frontend	Bundle 759 bytes, unchanged
50	Tenant C frontend	Bundle 759 bytes, unchanged

A.10 Container Identity Disclosure (5 items)

#	Disclosure	Source
51	Container app name	AUTH_SESSION_ID cookie
52	Container revision number	AUTH_SESSION_ID cookie
53	Deployment hash	AUTH_SESSION_ID cookie
54	Pod identifier	AUTH_SESSION_ID cookie
55	Internal port number	AUTH_SESSION_ID cookie

A.11 Injected Test Record Cleanup (id:9 through id:12)

#	Record	Evidentiary Status	Day 8 Status	Day 63 Status
56	Test record id:9 (`base_url` : empty string)	Corroborated by 2026-03-19 and 2026-03-24 reassessments and by contemporaneous research notes	Present in production database	Not externally verifiable (configuration endpoint returns 404 on retopologized prod APIM)
57	Test record id:10 (`base_url` : `https://deloitte.atlassian.net`)	Corroborated by 2026-03-19 and 2026-03-24 reassessments and by contemporaneous research notes	Present in production database	Not externally verifiable
58	Test record id:11 (`base_url` : tenant-controlled Jira hostname, FQDN redacted and available to coordinator)	Described in technical-delivery drafts of this finding; lacks contemporaneous HTTP capture in preserved evidence	Reported in field; not independently verified	Not externally verifiable
59	Test record id:12 (`base_url` : tenant-controlled Atlassian Cloud hostname, FQDN redacted and available to coordinator)	Described in technical-delivery drafts of this finding; lacks contemporaneous HTTP capture in preserved evidence	Reported in field; not independently verified	Not externally verifiable

---

End of Advisory

Zero|Tolerance Security Research
Coordinated Vulnerability Disclosure under CERT/CC VINCE / CISA VRC framework