

Penetration test report

Alderwick Industrial Supply

Customer portal & internal network

REPORT DATE

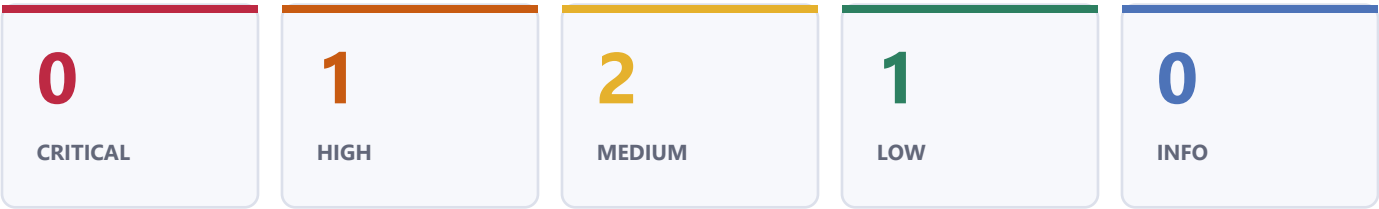
31 October 2026

ASSESSMENT WINDOW

26-30 October 2026

REFERENCE

AIS-2026-01



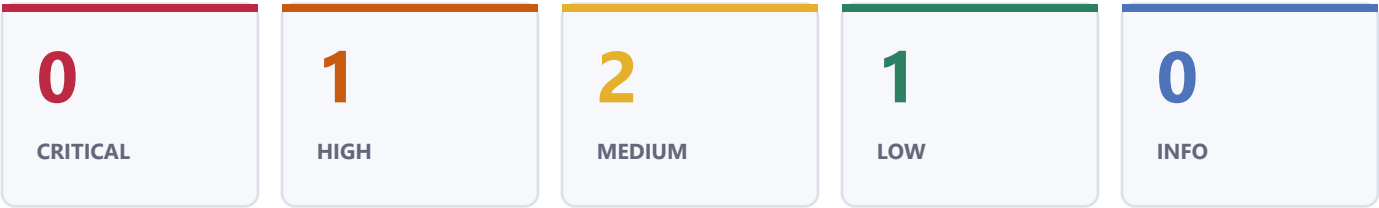
Four findings across application access controls, network segmentation, session recovery, and security logging.

IN THIS REPORT

Executive summary	02	Scope & methodology	03
Technical findings	04-07	Remediation & retesting	08

Executive summary

The highest-priority issue is cross-customer access to invoices in the customer portal. A signed-in account can request an invoice belonging to another customer without an ownership check.



Business impact and priorities

Invoice data exposes customer contact details, purchased items, and pricing. The access issue should be contained first, then corrected in the shared authorization layer. Three additional findings increase exposure or weaken recovery and investigation.

ID	FINDING	SEVERITY	PAGE
01	Cross-customer invoice access	High	04
02	Management interface reachable from user network	Medium	05
03	Existing sessions survive password recovery	Medium	06
04	Security log retention below policy	Low	07

RECOMMENDED FIRST ACTION

Restrict the affected invoice endpoint while the authorization fix is developed. Assign an application owner, review invoice-access logs, and retest with separate customer accounts before reopening access.

Scope & methodology

ASSESSMENT OBJECTIVES

Evaluate customer-to-customer data isolation, account recovery, administrative access boundaries, and the records needed to investigate misuse.

ASSET / BOUNDARY	COVERAGE
portal.alderwick.example	Two customer accounts; invoice access; password recovery and session lifecycle.
192.0.2.20:8443	Management console access from an employee-network test host and approved administration path.
Application & firewall audit records	Event coverage, access controls, and the retention configuration for the scoped systems.

APPROACH

Authenticated, manual testing used paired accounts and controlled requests to compare permitted and prohibited access. Network checks were limited to agreed hosts and ports. Configuration review supported the session and logging findings.

BOUNDARIES

No denial of service, phishing, credential spraying, persistence, or third-party systems were included. Results describe the listed assets during the assessment window; changes elsewhere require separate review.

SEVERITY LEGEND

Critical	Immediate, broad compromise with severe business impact.
High	Significant data or system exposure with a practical attack path.
Medium	Meaningful exposure with constraints or additional prerequisites.
Low	Limited direct impact; improves resilience or investigation.
Info	Observation without a demonstrated security impact.

Technical finding 01

High

STATUS: OPEN

Cross-customer invoice access

AFFECTED SYSTEM	CATEGORY
Customer portal / invoice API	Object-level authorization

The invoice API accepts a record identifier without verifying that the signed-in customer owns the requested invoice.

IMPACT

A customer account can read another customer's invoice, including contact details, line items, and negotiated pricing. The observed issue concerns read access; invoice modification and unauthenticated access were not established.

VALIDATION

1. Sign in as Customer A and request an invoice assigned to that account.
2. Keep the same session and request the known identifier of Customer B's invoice.
3. Compare the owner in the response with the customer attached to the session.

EVIDENCE

```
Session customer: CUST-A
GET /api/invoices/INV-B-1042
HTTP 200 OK
customer_id: CUST-B
invoice_total: 2,480.00
```

The response returned Customer B's invoice while the request used Customer A's session.

REMEDIATION

Enforce customer ownership in the server-side authorization layer for every invoice read and download. Scope database queries to the authenticated customer; reject mismatches before retrieving invoice content. Review equivalent endpoints for the same defect.

RETEST ACCEPTANCE

Customer A receives 403 or a non-disclosing 404 for Customer B's invoice and download. Customer B retains normal access. Repeat across at least two unrelated customer pairs.

APPLICATION ENGINEERING	Contain within 2 business days; fix within 7 days
-------------------------	---

Technical finding 02

Medium

STATUS: OPEN

Management interface exposed to the user network

AFFECTED SYSTEM	CATEGORY
192.0.2.20:8443 / management console	Network segmentation

The management console is reachable from the standard employee network, although access is intended to be limited to the administration network.

IMPACT

A compromised employee workstation gains a route to the management login surface. This broadens the opportunity for credential misuse or attacks against the console. No authentication bypass or administrative compromise was demonstrated.

VALIDATION

1. Connect from the approved employee-network test host.
2. Open the management interface on the agreed HTTPS port.
3. Compare the reachable path with the documented administration-only boundary.

EVIDENCE

```
Source zone: Employee network
Destination: 192.0.2.20:8443
TCP connection: established
HTTPS response: 200 OK
Page: Management console sign-in
```

The sign-in page was reachable from a network that should not have access to the management service.

REMEDIATION

Permit the management service only from the administration subnet or approved access gateway. Apply matching host and network rules. Keep multifactor authentication and individual administrator accounts in place.

RETEST ACCEPTANCE

Connection attempts from the employee network are denied or time out. The approved administration path remains available and requires normal authentication.

INFRASTRUCTURE OPERATIONS

Restrict access within 30 days

Technical finding 03

Medium

STATUS: OPEN

Existing sessions survive password recovery

AFFECTED SYSTEM	CATEGORY
Customer portal / account recovery	Session lifecycle

A session established before password recovery remains valid after the user completes the recovery flow, despite the account-recovery policy requiring all existing sessions to end.

IMPACT

An attacker who already holds a valid session can retain account access after the owner resets the password. Exploitation requires a pre-existing session; password reset alone does not grant access to another account.

VALIDATION

- 1. Establish Session A in one browser and start password recovery in another.
- 2. Complete the recovery flow and set a new password.
- 3. Use Session A to request the authenticated account page again.

EVIDENCE

```
09:12 Session A established
09:16 Password recovery completed
09:17 Session A -> GET /api/account
      HTTP 200 OK
      authenticated: true
```

The pre-recovery session remained authorized after the password was changed through account recovery.

REMEDIATION

Revoke active sessions and refresh tokens when account recovery succeeds. Require fresh authentication for subsequent requests and record the revocation event. Confirm that web, mobile, and API sessions share the same recovery policy.

RETEST ACCEPTANCE

Every pre-recovery session and refresh token fails after recovery. A new login with the new password succeeds. Test concurrent sessions and delayed refresh attempts.

APPLICATION ENGINEERING	Correct session revocation within 30 days
-------------------------	---

Technical finding 04

Low

STATUS: OPEN

Security log retention below policy

AFFECTED SYSTEM	CATEGORY
Portal and management audit records	Detection and investigation

Audit records are retained for seven days, below the organization's 90-day retention requirement. Older records were not available in the reviewed logging destinations.

IMPACT

An incident discovered more than a week after the event may lack the account, source, and administrative records needed to establish its timeline. This gap does not provide an access path by itself.

VALIDATION

- 1. Review the stated retention requirement for the scoped systems.
- 2. Inspect the configured retention in the application and central logging destinations.
- 3. Search for an approved historical event older than the current seven-day window.

EVIDENCE

Required retention: 90 days
Configured retention: 7 days
Oldest searchable record: 23 Oct 2026
Historical control event: unavailable

The configured retention and available records did not meet the documented investigation requirement.

REMEDIATION

Set retention to at least the agreed 90-day period, with capacity monitoring and access controls. Confirm that authentication, recovery, administrative, and invoice-access events reach the central store. Alert on interrupted ingestion.

RETEST ACCEPTANCE

Verify the retention setting, event delivery, and restricted deletion permissions. Confirm records remain searchable after seven days and again at the full retention boundary.

SECURITY OPERATIONS

Update retention within 60 days

Remediation & retesting

Close the invoice authorization gap first, then reduce management exposure and correct session recovery. Logging changes should proceed in parallel with application and network fixes.

ID / PRIORITY	ACTION & OWNER	TARGET
01 / High	Restrict invoice access; correct ownership checks. Application engineering	2-day containment 7-day fix
02 / Medium	Limit console access to the administration path. Infrastructure operations	30 days
03 / Medium	Revoke sessions after account recovery. Application engineering	30 days
04 / Low	Extend retention and verify event delivery. Security operations	60 days

TARGETS ARE MEASURED FROM REPORT DELIVERY

Retest record

Each finding remains open until the acceptance checks on its finding page pass. Record the build or configuration tested, the evidence reference, the result, and any remaining exposure.

FINDING	RETEST STATUS	ACCEPTANCE CHECK
01	Pending	Cross-customer reads denied; owner access preserved.
02	Pending	Employee path blocked; admin path operational.
03	Pending	Old sessions revoked; new authentication succeeds.
04	Pending	Retention, ingestion, access, and aging verified.