In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

Amadeus PSS Exposure and Shared-Platform Risk in Aviation

Verified exposure, distinct supplier incidents and practical resilience actions for aviation operators

Field	Detail
Classification	TLP:CLEAR – may be shared without restriction
Type	Sector advisory – third-party identity exposure and shared-platform resilience
Sector	Aviation: airlines, airports, ground handlers, passenger-processing and technology suppliers
Intended readers	CISOs, IT and OT security teams, airport operations, supplier management and data protection leads
Status	Public-source assessment as of 4 November 2026; affected-airline investigations continue

This advisory is community guidance. It is not a forensic finding, a compliance assessment or legal advice.

1. Bottom line

Airlines across Asia-Pacific have disclosed unauthorised access to passenger reservation data held by Amadeus. Airline notices describe use of credentials assigned to an Amadeus system account. JAL identifies traces within an August 2023–September 2026 window; this does not establish continuous access throughout that period. Published counts include JAL/JTA (about 92,000 customers), ANA (about 37,800 customers), Cathay Pacific (about 53,000 bookings) and Singapore Airlines (about 46,000 booking records). These different units must not be summed as unique individuals.[2, 3, 4, 5]

Separately, Amadeus acknowledged and remediated a vulnerability in a travel-booking display environment. Public evidence does not establish whether that issue is linked to the system-account incident. A separate Amadeus service interruption at Southwest Airlines on 9 October required manual baggage and boarding processing; no connection to the reservation-data exposure or a cyberattack was reported. No direct airport OT compromise has been established. OT-ISAC assesses the primary operational lesson as the need to understand supplier identity controls, integration dependencies and continuity arrangements.[1, 11]

Five priorities for aviation operators this week

1. Obtain written Amadeus/PSS scope confirmation, including affected accounts, records, dates and containment actions.
2. Preserve relevant logs and coordinate the revocation or rotation of affected service-account credentials and tokens with each provider.
3. Brief customers and contact-centre teams on potential booking-themed phishing; use verified airline channels for follow-up.
4. Review internet exposure of owned management, diagnostic and test environments; test third-party systems only with authorisation.
5. Confirm manual check-in, boarding, baggage and supplier-outage procedures; escalate relevant observations through established reporting routes.

2. What is known

Public statements establish a reservation-data access incident and a separately disclosed booking-display vulnerability. Whether the two issues are connected has not been established. They must not be merged into one confirmed attack chain.

Path	What was reported	Source
A. Amadeus system-account misuse	Cathay Pacific, Korean Air and Asiana report unauthorised access using credentials assigned to an Amadeus system account. JAL and ANA also confirm access to reservation data. Credential origin, attacker identity and full scope remain under investigation.	Airline disclosures [2–4, 6–7]
B. Booking-display exposure	Amadeus says a vulnerability affecting a travel-booking display environment allowed access to certain booking-display data. It says the vulnerability was fixed and monitoring enhanced. heise reported an accessible application memory dump; neither source establishes a link to path A.	Amadeus; heise [1, 10]

Timeline (newest first)

Date	Event
3 Nov 2026	Singapore Airlines discloses about 46,000 booking records involved; its own IT systems were not breached [5].
31 Oct 2026	Malaysia Airlines announces potential customer-information impact through Amadeus; no final record count [8].
28–30 Oct 2026	JAL/JTA, ANA, Cathay Pacific and Star Flyer disclose reservation-data exposure [2–4, 9].
23 Oct 2026	Korean Air and Asiana publish notices after notification by Amadeus on 20 October [6–7].
13 Oct 2026	heise reports a separately described booking-display/diagnostic-data exposure [10].
9 Oct 2026	Southwest Airlines reports an Amadeus service outage and manual bag/boarding processing [11].
1 Oct 2026	Amadeus publishes a statement on the booking-display vulnerability; it says remediation is complete [1].
10 Aug 2023–23 Sep 2026	JAL reports the window within which external access traces were identified; precise periods of activity remain uncertain [2].

Reported impact (APAC carriers)

Airline	Reported scale	Notable data types
Japan Airlines / JTA	About 92,000 customers	Booking reference, name, itinerary, class; roughly 2,000 had additional contact/passport-related fields [2].
ANA	About 37,800 customers	Approximately 1,700 with additional passport and contact information [3].
Cathay Pacific	About 53,000 bookings	Mostly booking reference, name and flight details; additional data possible for a smaller subset [4].
Singapore Airlines	About 46,000 booking records	About 620 records may include extra contact, travel-document and KrisFlyer data; no bookings reported altered [5].
Korean Air / Asiana	Count not yet confirmed	Reservation references reported; further fields and total scale under investigation [6–7].

Airline	Reported scale	Notable data types
Malaysia Airlines / Star Flyer	Count not yet confirmed	Potential booking-data exposure; operators assessing scope [8–9].

Evidence limits: the published counts refer to customers, bookings and records, not a deduplicated population. The means by which system-account credentials were acquired, any relationship to the display-environment issue, the complete airline scope and any unauthorised modification of records remain unresolved. No publicly verified Amadeus-to-airport-OT intrusion pathway was identified in the sources reviewed.

3. Why it matters beyond a data breach

On 9 October 2026, Southwest Airlines reported a brief system interruption at Amadeus and continued checking bags and boarding passengers manually. Flight-tracking reports recorded more than 1,200 flight delays and around 40 cancellations during the disruption; these figures do not prove that every disruption was solely caused by the outage. Amadeus attributed the technical issue to another technology provider. No link to the passenger-data incident or to malicious activity has been established. [11, 12]

JAL and Cathay Pacific said flight operations were unaffected by the reservation-data incident; Singapore Airlines stated its own IT systems were not breached and that no bookings were modified. These statements should not be extended to every airline without confirmation. [2, 4, 5]

- **Booking-themed phishing.** Authentic reservation details could make fraudulent messages more persuasive. This is a plausible downstream risk, not a confirmed campaign using the disclosed records.
- **Travel-document and privacy risk.** A smaller subset of reported records included travel-document or contact information; organisations should assess notification and fraud risks in relevant jurisdictions.
- **Reservation integrity.** Read access does not automatically imply write access. Check for unexplained changes where logs and permissions allow; SIA reported no changes to affected bookings. [5]
- **Shared-service concentration.** The separate September 2025 Collins Aerospace MUSE ransomware incident disrupted passenger-processing functions at several European airports, demonstrating that shared service loss can require manual fallback. It is not evidence of compromise from this Amadeus event. [13]
- **Provider-side visibility.** The reported access window highlights the value of service-account ownership, anomaly detection and prompt supplier notification; public sources do not establish the exact duration of continuous access or a specific monitoring failure.

4. Confirmed incidents and defensible lessons

The events below demonstrate different risks–credential misuse, a separately disclosed application exposure, ransomware and an availability outage. They are not a single campaign, and none establishes direct compromise of airport OT in the Amadeus incident.

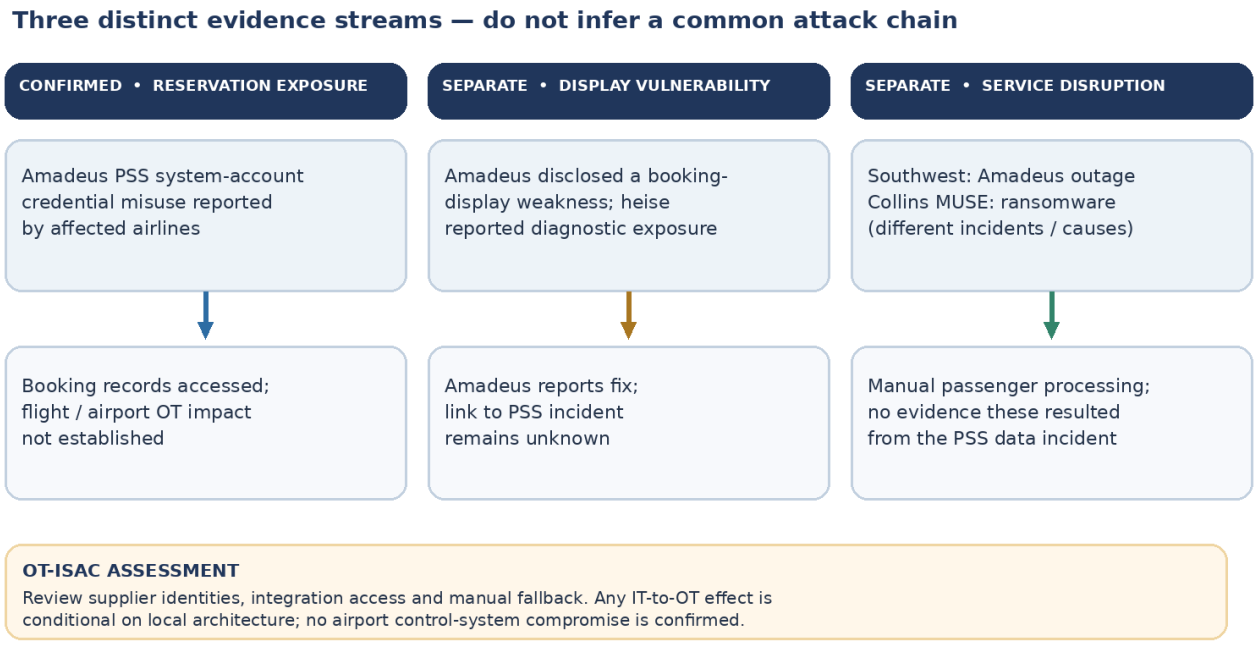

Figure 1. Distinct evidence streams and an illustrative supplier-dependency assessment; no causal link between the separate incidents is established.

Selected incidents and evidence (newest first)

Date	Incident	How access was gained	Operational impact
Nov 2026	Singapore Airlines / Amadeus PSS	Reservation data accessed at supplier; identity exposure details under investigation	About 46,000 booking records; airline systems not breached; no reported booking modifications [5]
Aug 2023–Sep 2026	Amadeus PSS access window	Use of an Amadeus system-account credential, per airline notices	Customer reservation data exposure; no verified airport OT impact [2–4, 6–7]
Oct 2026	Amadeus booking-display vulnerability	Amadeus acknowledges separate booking-display weakness; heise reports diagnostic data exposure	Potential booking-display data access; linkage to PSS credential misuse unknown [1, 10]
9 Oct 2026	Southwest / Amadeus outage	Service interruption attributed to a third-party technology provider; no cyberattack reported	Manual bag and boarding processing; national flight-status delays reported [11–12]
Sep 2025	Collins Aerospace MUSE (Europe)	Ransomware affecting a shared passenger-processing supplier	Manual processing and flight disruption at several European airports [13]
Mar 2025	Kuala Lumpur International Airport	Cybersecurity incident reported by Malaysian authorities; actor not confirmed	NACSA and Malaysia Airports stated airport operations were unaffected; other disruption claims disputed [14]

Classification: vendor/airline notices and authoritative reporting are treated as confirmed for the facts they state. Separate mechanisms, unverified criminal claims and claimed operational impacts are not assumed to be causally linked.

Six lessons for operators

1. **Provider identities are part of the attack surface.** The system-account misuse described by airlines supports reviewing service-account rights, oversight and unusual bulk access.
2. **A shared provider can concentrate exposure.** One platform can process many organisations' records even when their own corporate systems are not breached.
3. **Diagnostic environments deserve separate attention.** Amadeus acknowledged a booking-display vulnerability; its relationship to the reservation-data incident remains unproven.

4. **Distinguish cyber incidents from outages.** Southwest's October service interruption and the Collins MUSE ransomware incident had different known causes.
5. **Long reporting windows are not proof of continuous dwell.** Validate access periods, retained logs and the provider's detection timeline before claiming persistent attacker activity.
6. **Manual fallback requires coordination.** Airports, airlines and handlers should exercise check-in, boarding, baggage and passenger-communications dependencies, including staffing.

OT-ISAC assessment: these examples justify targeted supplier assurance, identity monitoring and continuity exercises. They do not establish a general attack-frequency trend or a verified compromise of airport control networks.

5. Aviation systems with related dependency risks

The following are review dimensions, not confirmed weaknesses in any named airline or airport. Apply them only where asset inventory, architecture and supplier evidence show the condition exists:

- **P1 Shared platform** – a vendor, integration or service supports multiple operators or sites.
- **P2 Long-lived identities** – service accounts, API credentials or privileged integrations are not adequately bounded, monitored or rotated.
- **P3 Diagnostic/non-production exposure** – test, display, logging or administrative systems could expose live data or secrets.
- **P4 Supplier-held access** – third-party support privileges or network paths are not fully inventoried or time limited.

Consequences below are illustrative and conditional. Higher operational or safety risk depends on whether a shared identity or supplier connection can reach the relevant airport network and affect availability or integrity; no such pathway is confirmed in the Amadeus exposure.

Layer	System or equipment	Patterns	If misused	Check first
Commercial	Reservations / passenger service systems; GDS	P1 P2 P3 P4	Possible access to booking data or disruption of reservations	Validate vendor scope, assigned accounts, log access and remediation
Commercial	Departure control systems: check-in, boarding, load control	P1 P2 P4	Potential passenger-processing or data-integrity disruption	Review integration permissions and booking/load-data change controls
Commercial	Loyalty, alliance and booking-data partners	P1 P2	Potential cross-partner data exposure	Map recipients, contracts and notification commitments
Commercial	Contact centres, CRM and travel-agent portals	P1 P2	Possible account takeover or targeted customer fraud	MFA, fraud indicators and unusual export monitoring
Passenger processing	Common-use check-in and boarding platforms	P1 P4	Availability loss may require manual processing	Vendor path inventory and tested offline procedures
Passenger processing	Kiosks, self bag-drop and biometric gates	P1 P2 P4	Possible queue and passenger-processing disruption	Shared endpoint images, administrative access and failover
Airport operations	AODB, resource allocation, flight-information displays	P1 P2 P4	Possible inaccurate information or loss of services	Integration inventory, logging, read/write privileges
Airport OT	Baggage handling controls (PLC/SCADA and interfaces)	P2 P4	Potential stoppage only if access path reaches control network	Integrator paths, engineering accounts, segmentation, backups
Airport OT	Boarding bridges, ground power, airfield lighting	P2 P4	Potential operational/safety implications; system dependent	Safety-approved change control and vendor-access pathways
Airport OT	BMS, access control and fuel monitoring	P2 P4	Possible availability or integrity effects if connected	Test network separation and remote-access restrictions
Airline operations	Operations control, crew and maintenance back ends	P1 P2 P4	Possible scheduling or information-integrity impact	Bound service accounts and monitor critical integration changes

Layer	System or equipment	Patterns	If misused	Check first
Cross-cutting	Web/API management interfaces; staging and test copies	P2 P3	Possible exposure of credentials or operational data	Authorised external exposure checks and secure environment configuration

Airport OT systems need a separate engineering-led assessment. Mapping third-party access and IT-to-OT trust boundaries is prudent, but this Amadeus incident has not been shown to compromise baggage controllers, boarding bridges, AGL, fuel systems or safety functions.

6. Action items

These measures prioritise safe, evidence-led checks; operational technology testing or change must follow site and vendor approval and aviation safety procedures.

When	Action	Lead	Support
This week	Request written incident scope from Amadeus/PSS and other relevant suppliers: identities, records, dates, containment, residual access and notification.	Vendor management	CISO; DPO
This week	Preserve available authentication and API logs; coordinate rotation/revocation of affected service credentials and tokens without breaking passenger-processing integrations.	IT security	Vendor; operations
This week	Prepare booking-themed phishing advice for staff and affected travellers. Use confirmed airline notices and official verification channels.	Customer service	Comms; security
This week	Inventory and review internet-facing management, debug and test services you own. Test vendor-hosted environments only with written authorisation.	IT security	Application owners
This week	Assess applicable privacy notification duties and coordinate customer communication with the data owner and legal team.	DPO / Legal	CISO
30 days	Create a register of privileged identities, APIs, service accounts and vendor dependencies, with owners, purpose, scope and rotation controls.	IT security	Vendor management
30 days	Review available PSS logs for anomalous bulk reads, unusual identities and unexplained booking changes; obtain vendor evidence where logs are not locally available.	SOC / IT security	PSS vendor
30 days	Map vendor remote-access paths into baggage, bridge, building and airfield systems; enforce least privilege and time-limited access after OT review.	OT engineering	IT; procurement
30 days	Confirm a coordinated, safety-approved manual-processing plan for check-in, boarding, bag drop and baggage handling during supplier outages.	Airport operations	Airlines; handlers
90 days	Update vendor contracts for defined incident-notification timelines, security evidence, customer audit information and restrictions on production data in non-production environments.	Procurement / Legal	CISO; DPO
90 days	Exercise a supplier outage or account misuse scenario with airlines, ground handlers and airport teams; measure time to stable manual operations.	Risk / BCM	Operations; security
90 days	Review vendor monitoring for unusual system-account activity, root-cause updates, reassessment triggers and tested recovery dependencies.	CISO	Vendor management

For smaller teams

Start with three things: confirm whether your records or accounts were affected, protect the relevant credentials without interrupting operations, and rehearse manual passenger processing with your supplier.

7. Monitoring, reporting and external enquiries

Report credible indicators through your organisation’s security incident process, notify the affected supplier, and assess any regulator or privacy reporting obligations. Operators may also contact OT-ISAC with non-sensitive sector observations through its published public contact channel.

Indicators worth investigating

- A vendor notice identifying impacted passenger data, credentials or an unexplained change to scope.
- Unusual service-account logins, source locations, bulk queries or changes in API permissions.
- Booking or itinerary amendments inconsistent with authorised staff and customer activity.
- Suspicious messages referencing authentic booking information or requesting sensitive details.
- Known leaked credentials or active tokens associated with relevant supplier integrations.
- Management, diagnostic or test environments exposed to networks that do not require access.
- Unexpected vendor sessions or cross-zone traffic into airport operational networks.

Suggested escalation routes

Who to contact	Suggested information or next step
PSS / technology supplier	Confirm affected identities, data scope, access evidence, remediation and monitoring measures
Internal IT security / SOC	Preserve logs; review service accounts, booking changes and external exposure
Airport and airline operations	Coordinate manual processing and supplier-outage readiness
DPO / relevant authority	Assess notification and regulatory obligations in each affected jurisdiction
OT-ISAC (voluntary)	Share generalised observations or request public-facing information via info@otisac.org [15]

Information shared with OT-ISAC is voluntary and does not replace legal, regulatory or contractual reporting obligations. Do not send passenger personal data, credentials or sensitive system details through general email. Confirm appropriate handling and classification before sharing.

Public enquiries: info@otisac.org | https://www.otisac.org/contact

8. Public sources and assessment limitations

Source cut-off: 4 November 2026 (SGT). Confirmed facts are attributed to originating airlines, Amadeus or named authorities. OT-ISAC assessments and scenario consequences are explicitly conditional. Figures can change; no forensic access or undisclosed airline/airport asset inventory was available for this public report.

[1] Amadeus – Data and Vulnerability Statement (October 2026): https://amadeus.com/en/industry-messaging/amadeus-statement-oct

[2] Japan Airlines – Unauthorized Access to Amadeus Passenger Service System (28–29 Oct 2026): https://www.jal.co.jp/en-jp/news/general/2026/other/261028.html

[3] All Nippon Airways – Unauthorized Access to Passenger Service System Provided by Amadeus (30 Oct 2026): https://cad.www.ana.co.jp/en/jp/special-notice/001613.html

[4] Cathay Pacific – Personal data security incident involving third-party provider (30 Oct 2026): https://www.cathaypacific.com/cx/it_IT/latest-news/security-and-operational-changes/personal-data-security.html

[5] Channel NewsAsia – Singapore Airlines statement on 46,000 booking records (3 Nov 2026): https://www.channelnewsasia.com/singapore/sia-singapore-airlines-amadeus-data-breach-booking-records-6517151

[6] Korean Air – Official Amadeus customer notice (23 Oct 2026; Korean): https://www.koreanair.com/contents/footer/customer-support/notice/2026/amadeus

[7] Asiana Airlines – Official Amadeus customer notice (23 Oct 2026; Korean): https://flyasiana.com/C/KR/KO/customer/notice/detail?id=CM202610230002530882

[8] Malaysia Airlines – Cybersecurity Incident Involving Third-Party Technology Provider (31 Oct 2026): https://www.malaysiaairlines.com/my/en/mh-media-centre/important-for-you/cybersecurity-incident-third-party-technology-provider.html

[9] Star Flyer – Unauthorized Access to Amadeus PSS notice (30 Oct 2026): https://www.starflyer.jp/en/news/2026/news_20261029_info.html

[10] heise online – Security vulnerability in flight-booking system (13 Oct 2026; German): https://heise.de/-11479912

[11] Southwest Airlines – Returns to Normal Operations After Vendor System Outage (9 Oct 2026): https://www.swamedia.com/news-and-stories/update/southwest-returns-to-normal-operations-after-vendor-system-outage-MCNGRABJ547FGMHIGWBB7GD6TFQM

[12] KERA / Texas Public Radio – Southwest flight status during supplier outage (10 Oct 2026): https://www.tpr.org/economy-and-labor/2026-10-10/more-than-1-200-southwest-airlines-flights-delayed-after-software-outage

[13] Reuters – ENISA confirmation of Collins Aerospace ransomware-related airport disruption (22 Sep 2025): https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/

[14] The Star – NACSA and Malaysia Airports joint statement, KLIA operations unaffected (25 Mar 2025): https://www.thestar.com.my/news/nation/2025/03/25/klia-operations-not-affected-by-cyber-attack-says-nacsa-and-mahb

[15] OT-ISAC – Public contact information: https://www.otisac.org/contact

About this advisory

Prepared by OT-ISAC for aviation and critical-infrastructure stakeholders in Asia-Pacific using publicly available information. TLP:CLEAR – unrestricted sharing is permitted. Analytical judgements are identified, and guidance is not a compliance assessment, legal advice or a forensic conclusion.