LH-SBS-WR —Weekly Status Report —Week 36 LHN-8007·

WEEKLYSTATUSREPORT

Week 36—August 31 – September 4, 2026

The Dash —SBS's Multi-Gated AI Orchestrator Platform

Document Title	Weekly Status Report — Week 36 (August 31 – September 4, 2026)
Document Type	Report
Document Series	LH-SBS-WR
Reference	LHN-8007
Version	V1.0
Date	September 4, 2026
Reporting Period	Monday, August 31 – Friday, September 4, 2026 (ISO Week 36, period ending September 4, 2026)
Author	Frank Yglesias, Chief Executive Officer and Acting Project Manager, Ledger Hub Networks, LLC
Prepared For	Nelson Santos, IT Director, Spanish Broadcasting System, Inc.
Classification	Confidential
Status	Final

Revision History

Version	Date	Author	Change Summary
V1.0	September 4, 2026	F. Yglesias	Initial issue — Week 36 weekly status report

List of Acronyms

Acronym	Expansion
API	Application Programming Interface
CORS	Cross-Origin Resource Sharing
CSS	Cascading Style Sheets
DoS	Denial of Service
E2E	End-to-End
HTML	HyperText Markup Language
IAM	Identity and Access Management
JWT	JSON Web Token
LHN	Ledger Hub Networks
MD	Markdown
PAN	Primary Account Number
PDF	Portable Document Format
PII	Personally Identifiable Information
PoC	Proof of Concept
SSH	Secure Shell
TLS	Transport Layer Security
UFW	Uncomplicated Firewall
UI	User Interface
VPN	Virtual Private Network

1 Reporting Period and Scope

This report covers Ledger Hub Networks, LLC (LHN) delivery activity for ISO Week 36, August 31 – September 4, 2026, period ending September 4, 2026, under reference LHN-8007. Scope is limited to the LaMusica / SBS Payments System Security Audit — a pivot from infrastructure auditing to code-level auditing of the **`payment-center`** and **`payment-center-admin-client`** repositories after the development team revoked SSH access to production servers. The audit was conducted in read-only mode on production; all changes were implemented in a local branch and validated on a secure staging environment deployed from scratch. Three new critical vectors were discovered, a per-endpoint remediation plan (F1–F6) was written, security patches were implemented and validated, and the Converge merchant portal was audited from the inside. All findings were documented with evidence and delivered

to Nelson Santos, IT Director, Spanish Broadcasting System, Inc.

2 Work Completed — Week 36

Five workstreams were completed during the reporting period:

Item	Workstream	Detail
WR36-01	Access Lockout and Per-Endpoint Remediation Plan	The development team revoked SSH access to **DO-STIMPY** and **DO-REN** and disabled services; the audit key is no longer in effect. Drafted a requirements list for the board of directors (7 items: read-only repos, PR history, CI/CD docs, read-only SSH to STIMPY, service reactivation, access logs, and a technical point of contact) — **reportes/solicitud-acceso-auditoria-pagos-2026-08-31.md**. Cloned **payment-center** (backend + client) and **payment-center-admin-client** into **reposPayments/** (**master-do** branch). Local working branch **audit/security-remediation**; no commits or pushes by explicit order. Completed code mapping (**00-mapeo-proyectos-2026-08-31.md**) and drafted the F1–F6 remediation plan (~12.5–13.5 h, security patches only): F1 transactions (H1/H2/H19), F2 representatives + anonymous DELETE, F3 change-password, F4 profiles/:id whitelist, F5 frontend verification, F6 regression/evidence. Executive PDF in LHN format (4 pages) in **reposPayments/report-auditory/**. System viability analysis documented in **02-viabilidad-sistema-2026-08-31.md**.
WR36-02	Diagrams, Secure Staging and Payment-Flow Verification	Produced architecture diagrams for payment-center (archify, ES/EN): overall architecture and 2-repo flow, with Converge/Elavon marked as a risk zone (PIN in git, no webhooks), plus "after the change" versions. F1–F4 fixes implemented in the local branch working tree and validated with regression evidence (**03-evidencia-regresion-2026-09-01.md**). Documented decision: **profiles/:id** stays public with a 10-field whitelist. Staging deployed from scratch on droplet **161.35.108.98** with the remediated branch: **payments.sbsdash.com** (Express API behind nginx), **devp.sbsdash.com** (Vue client) and **adminp.sbsdash.com** (admin with basic auth), all 3 with TLS. MongoDB 7 with auth and localhost **bindIp**, UFW, a new 64-hex JWT secret (the original was weak and shared), production profiles neutralized against accidental startup, everything in demo mode. H15 closed: there is no Converge webhook receiver; the Elavon flow is 100% synchronous (embedded SDK browserElavon: the PAN never touches our server or Mongo). Authorized test of production credentials: $1 token request against production Elavon answers 403; the leaked secret can no longer charge. Reverted to demo in ~1 minute, zero money moved. Real $1 payment attempt through the UI (real card, staging pointing at production): same merchant failure **java.sql.SQLException: Year out of range** — no charge made. Staging users created: 3 admins + 1 payment test user.
WR36-03	Architecture Diagram Publication	Published **paymentflow.sbsdash.com** as a static site serving the payment-center architecture diagram (EN version) for team reference. Deployed via the canonical sbsdash pipeline: rsync to **/var/www/paymentflow.sbsdash.com**, Caddy block with TLS, favicon from **ceo.sbsdash.com**, **caddy validate + reload**. Verified: certificate Let's Encrypt production, 0 external references, render OK.
WR36-04	Converge (Elavon) Portal Audit	Inside audit of the Converge merchant portal with 36 evidence screenshots (**elavon-coverge/report-2026-09-03/**): Payments (current batch, declined transactions — 4 pages, settled batches, new-payment form); Product catalog and options; Employees and permissions — 6 accounts reviewed (**webpage**, **sbsapi**, **vvaquedano**, **credit**, **sbsweb**) with per-user rights detail, including transaction and user-management rights; Configuration — fraud rules (standard and custom), API security, system setup, hosted payments and payment fields. EN report with the LHN design system: **converge-audit-2026-09-03.en.pdf**.

Item	Workstream	Detail
WR36-05	Full Ecosystem Diagram	Produced an interactive diagram of the LaMusica/SBS ecosystem (archify, ES/EN): users and apps, the DO production fleet (7 droplets), the payments plane (payment-center, auth, SendGrid, Converge/Elavon, RevenueCat, Stripe, PayPal, Ebanx, ticket offices), the data plane (MongoDB Atlas, Spaces, legacy MySQL) and the cloud/code/IAM plane (Bitbucket, GitHub, GoDaddy, Cloudflare, AWS, Firebase/GCP, Elastic, ACRCloud, AI APIs). Deliverable at `archify-report/lamusica-ecosystem.{html,en.html}`.

3 Planned Work — Week 37 (September 7–11, 2026)

Four workstreams are planned for the next reporting period:

Item	Workstream	Detail
WR37-01	Production Deployment of F1–F4 Authentication Fixes	Deploy the validated F1–F4 security patches from the staging environment to production (`DO-STIMPY`). F1: authenticate `GET /api/transactions/client` endpoint (H1/H2/H19). F2: protect `DELETE /api/representatives` from anonymous deletion. F3: require valid token on `POST /api/auth/change-password`. F4: enforce 10-field whitelist on `GET /api/profiles/:id`. Coordinate with the development team for deployment window and rollback procedures. Validate with E2E smoke tests post-deploy.
WR37-02	Access Log Analysis and Exploitation Assessment	Obtain access logs for `payments.spanishbroadcasting.com` from the development team to determine whether the unauthenticated `/api/transactions/client` endpoint was already exploited in the wild. Correlate timestamps with the 39,298 transactions in the `payment_center` MongoDB cluster. Document findings and escalate if evidence of active exploitation is found.
WR37-03	Password Reset Campaign for 7,403 Compromised Users	Execute a forced password reset for all 7,403 users whose bcrypt cost-5 hashes were exposed via the unauthenticated API. The cost-5 hashes are mass-crackable with GPUs; preemptive rotation is mandatory. Design a secure reset flow (tokenized email links, 72-hour expiration, single-use) and validate deliverability via SendGrid before broadcast.
WR37-04	Formal Audit Channel and Board Engagement	Continue the audit through the formal channel (board of directors) after the development team revoked SSH access. Present the F1–F6 remediation plan, the 3 new critical vectors, and the Converge portal audit findings to the board. Request: read-only repo access, PR history, CI/CD documentation, read-only SSH to STIMPY, service reactivation, access logs, and a designated technical point of contact.

4 Decisions of Record

DoR-1—Read-Only Production, Changes Only in Local Branch and Staging

Date: August 31, 2026

After the development team revoked SSH access to production servers, the audit pivoted to code-level analysis with a strict separation: read-only on production, changes only in a local branch (`audit/security-remediation`), and validation only on secure staging. No commits or pushes were made to any remote by explicit order. The staging environment (`161.35.108.98`) was deployed from scratch with the remediated branch, neutralized production profiles, a new 64-hex JWT secret, and everything in demo mode. This decision ensures zero production risk while enabling full validation of security patches.

DoR-2—Staging as Mandatory Gate Before Production

Date: September 1, 2026

The secure staging environment on **`161.35.108.98`** is designated as the mandatory validation gate for all payment-system security patches before any production deployment. The staging topology mirrors production: Express API behind nginx (**`payments.sbsdash.com`**), Vue client (**`devp.sbsdash.com`**), admin panel with basic auth (**`adminp.sbsdash.com`**), all with TLS. MongoDB 7 with auth and localhost **`bindIp`**, UFW active. No patch may reach **`DO-STIMPY`** without passing regression tests, PoC verification, and user approval on staging. The F1–F4 fixes were validated on staging and are ready for production integration.

DoR-3—F1–F4 Authentication Fixes Take Absolute Priority

Date: September 1, 2026

The three new critical vectors discovered during code auditing take absolute priority over all other work: (1) F1 — unauthenticated **`GET /api/transactions/client`** exposing 39,298 transactions with customer PII (H1/H2/H19). (2) F2 — anonymous **`DELETE /api/representatives`** allowing representative deletion without auth (**`representatives.js:102`**). (3) F3 — tokenless **`POST /api/auth/change-password`** accepting **`{userID, password}`** and allowing account takeover (**`auth.js:292`**). (4) F4 — **`GET /api/profiles/:id`** without authentication exposing PII; decision to keep it public with a 10-field whitelist. These four fixes were implemented and validated on staging. No other infrastructure or feature work may proceed until F1–F4 are deployed to production and verified.

DoR-4—Leaked Production Credentials Verified Dead

Date: September 1, 2026

An authorized test of the leaked production Elavon credentials was conducted on staging: a $1 token request against the production gateway returned **`403 Forbidden`** from Elavon, confirming the leaked secret can no longer charge. The test was reverted to demo mode in approximately 1 minute with zero money moved. A real $1 payment attempt through the UI (real card, staging pointing at production) produced the same merchant failure **`java.sql.SQLException: Year out of range`** — no charge was made. The Elavon demo gateway is also broken (every sale fails with the same error). Decision: the leaked credential risk is mitigated (Elavon revoked it), but the broken demo gateway blocks payment-flow testing and must be escalated to Elavon support.

5 References

• LH-SBS-INF-001—Infrastructure Specification for The Dash (target and as-built states; verification gates)

• LH-SBS-SEC-001 V1.0—Security and Access Control Specification (36 controls, 8 families)

• LH-SBS-WR-0035—Weekly Status Report — Week 35 (LHN-8006)

• LH-SBS-SDD-001—Software Design Document — NornGate Agent Registry & Multi-Gated Orchestrator

• reportes/solicitud-acceso-auditoria-pagos-2026-08-31.md—Board requirements for audit access

• reposPayments/report-auditory/00-mapeo-proyectos-2026-08-31.md—Code mapping

• reposPayments/report-auditory/plan-remediacion-endpoints-2026-08-31.{html,pdf}—F1–F6 remediation plan (ES/EN)

• reposPayments/report-auditory/02-viabilidad-sistema-2026-08-31.md—System viability analysis

- reposPayments/report-auditory/03-evidencia-regresion-2026-09-01.md—Regression evidence (F1–F4)
- reposPayments/report-auditory/04-despliegue-staging-sbsdash-2026-09-01.md—Staging deployment report
- reposPayments/report-auditory/diagramas/—Architecture and repo flow diagrams (ES/EN, current and "after")
- elavon-coverge/report-2026-09-03/—Converge portal audit (EN PDF + 36 screenshots)
- archify-report/lamusica-ecosystem.{html,en.html}—Full ecosystem diagram

6 Change Register

Entry	Date	Change
CR-01	September 4, 2026	Initial issue — no prior edits.

Confidential —Ledger Hub Networks, LLC × Spanish Broadcasting System,
September 4, 2026