LH-SBS-WR —Weekly Status Report —Week 35 LHN-8006·

WEEKLYSTATUSREPORT

Week 35—August 24–28, 2026

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

Document Title	Weekly Status Report — Week 35 (August 24–28, 2026)
Document Type	Report
Document Series	LH-SBS-WR
Reference	LHN-8006
Version	V1.0
Date	August 28, 2026
Reporting Period	Monday, August 24 – Friday, August 28, 2026 (ISO Week 35, period ending August 28, 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	August 28, 2026	F. Yglesias	Initial issue — Week 35 weekly status report

List of Acronyms

Acronym	Expansion
API	Application Programming Interface
CFS	Commercial Free Station
CORS	Cross-Origin Resource Sharing
CVV	Card Verification Value
DoS	Denial of Service
DO	DigitalOcean
HTML	HyperText Markup Language
ISO	International Organization for Standardization
PAN	Primary Account Number
PDF	Portable Document Format
PII	Personally Identifiable Information
PoC	Proof of Concept
SSH	Secure Shell
TLS	Transport Layer Security
UI	User Interface
WP	WordPress

1 Reporting Period and Scope

This report covers Ledger Hub Networks, LLC (LHN) delivery activity for ISO Week 35, August 24–28, 2026, period ending August 28, 2026, under reference LHN-8006. Scope is limited to the LaMusica / SBS Infrastructure Security Audit on DigitalOcean — a comprehensive read-only assessment of the entire DigitalOcean account including console inventory, all 7 droplets, all 5 Spaces buckets, accessible MongoDB Atlas databases, and the Elavon/Converge payments stack. Two active compromises were confirmed during the audit: PHP webshells on the WordPress server and an unauthenticated payments API exposing customer PII. A 3-day remediation plan was drafted and a cost-saving resize plan was validated with 14 days of telemetry. All findings were documented with evidence and delivered to Nelson Santos, IT Director, Spanish Broadcasting System, Inc.

2 Work Completed — Week 35

Five workstreams were completed during the reporting period:

Item	Workstream	Detail
WR35-01	DigitalOcean Console Audit and Full Account Inventory	Completed a full read-only inventory of the "LaMusica Team" DigitalOcean account. Discovered 7 droplets across NYC1/NYC3, 5 Spaces buckets in NYC3 (~5.2 TiB), one 2 TB volume, and monthly spend of ~$2,700–3,700 (~$38,900/yr). Architecture is 100% classic: no Kubernetes, no load balancers, no cloud firewalls or DBaaS. Production database lives in MongoDB Atlas (external to DO); DNS is outside DO. Role map established: **DO-REN** = public web **lamusica.com** (80M req/mo, 77% cache hit); **DO-STIMPY** = CMS + chat + payments + assets; **DO-LAMUSICA-WP** = WordPress (78% CPU, 82% RAM); **DO-LAMUSICA-WAVE** = StreamCentral streaming; **ubuntu-c-8-nyc1** = streamcentral-clips development; **HITZMAKER** and **COMMERCIAL-FREE-STATION** idle. Deliverable: **auditoria-digitalocean.md**.
WR35-02	Droplet Security Audit — REN, STIMPY, ubuntu-c-8-nyc1	First inside-out audit over SSH with a temporary audit key. 8 critical findings documented: (1) Plaintext MongoDB Atlas credential shared by 7 apps on REN and STIMPY — urgent rotation required. (2) SSH brute force ~6,500 attempts/day on REN (6,821) and STIMPY (6,193); **PermitRootLogin yes** + **PasswordAuthentication yes**, no fail2ban. (3) **assets.lamusica.com** (82 GB) served only by Varnish cache — Apache dead since 2026-03-22, 0 origin requests in 5 months. (4) 13 Spaces keys all read/write/delete (1 master key for all buckets); 7 orphaned. (5) Wildcard CORS * on 4/5 buckets; access logs off on all 5. (6) 4/7 droplets without backups; the 2 TB volume without snapshots. (7) GitHub token in **/root/.git-credentials** and the streamcentral-clips repo under a personal GitHub account. (8) DO account 2FA codes in plaintext on the workstation. Contrast: **ubuntu-c-8-nyc1** had the best SSH config in the fleet (keys only, UFW deny-default, 0 effective attacks) — destroyed by Denis Vaque on 2026-08-26, the day after its audit. Deliverables: individual ES/EN reports in **reportes/**.
WR35-03	Payments Stack Audit — Elavon/Converge	Read-only audit of **payment-center** on DO-STIMPY (**payments.spanishbroadcasting.com**, Elavon's Converge gateway). Confirmed the **GET /api/transactions/client** endpoint is completely unauthenticated, exposing customer PII, truncated PANs, expirations, and bcrypt cost-5 hashes (mass-crackable with GPUs). Full MongoDB Atlas backup to local: **payment_center** cluster (39,298 transactions, 80,418 orders, 59,167 invoices, 7,403 users, 127 representatives, 13 markets) and the **lamusica/transcoding** cluster. Deliverables in **report-2026-08-26/**: payments audit report (ES/EN), security remediation plan (ES/EN), and a 2-page executive management brief (EN).
WR35-04	Remediation Plan and Live Proof-of-Concept	Drafted a 3-day remediation plan (nothing executed) for the critical payments findings, with ES/EN versions in MD and PDF under the Ledger Hub Networks, LLC brand. H4 resolved: PAN + Luhn scan over ~190k backup documents confirms the 39,298 transactions hold masked cards (**##********####**); no full PAN or CVV stored. New finding H18: 14 full PANs written into wrong fields. Live PoC (H19): unauthenticated customer-data theft reproducible in 30 seconds with **curl**; search **?q=gmail** 503 after 60s = unauthenticated DoS vector. Document with full attack chain and rebuttal table in **reportes/poc-exposicion-api-pagos-2026-08-28.md**. Documented plan to regain access to the 4 droplets not yet auditable (WAVE, HITZMAKER, CFS, WP).

Item	Workstream	Detail
WR35-05	Full Fleet Audit — Buckets, Databases, and Remaining 4 Droplets	Completed 100% account coverage. 5 Spaces buckets audited one by one (inventory, PII, CORS, logging) and 3 accessible MongoDB databases — ES/EN reports in **`report-2026-08-28/`**. DO-LAMUSICA-WP: active compromise confirmed — 8+ obfuscated executable PHP webshells in **`sbsmultisite`** uploads (HTTP 200 invoked), exfiltratable **`wp-config.php.bak`**, 1.14 GB SQL dump publicly downloadable, 111k SSH brute-force attempts in 7 days. DO-HITZMAKER: plaintext credentials committed to Git (Mongo Atlas, AWS, Elastic, Firebase Admin), **`POST /webhooks/vod`** without real auth, Node 16 EOL. DO-COMMERCIAL-FREE-STATION: public unauthenticated **`/admin/*`** endpoints, ingest port TCP 8000 open to Internet, dead TLS renewal (expires 2026-10-21). DO-LAMUSICA-WAVE: StreamCentral with 49 active stations across 10 markets and 2.01 TiB of recordings to the **`lamusica-wave`** bucket. DO account audit log (890 events, 2023-07-11 2026-08-28) reviewed via console. Consolidated delivery: **`pdfs-reports-2026-08-28/`** with 14 PDFs (7 servers × ES/EN): REN 7p, STIMPY 7p, ubuntu-c-8-nyc1 4p, WAVE 129p, WP 97p, HITZMAKER 126p, CFS 107p.

3 Planned Work — Week 36 (August 31 – September 4, 2026)

Four workstreams are planned for the next reporting period:

Item	Workstream	Detail
WR36-01	Execute 3-Day Remediation Plan for Payments API	Implement the drafted 3-day remediation plan for the critical payments findings: authenticate the **`GET /api/transactions/client`** endpoint, rotate the shared MongoDB Atlas credential, patch the bcrypt cost-5 hashes, and close the unauthenticated DoS vector (H19). Coordinate with 4 senior developers and validate each fix with regression tests before livenet deployment.
WR36-02	Droplet Hardening and Credential Rotation	Execute SSH hardening across all 7 droplets: disable **`PermitRootLogin`** and **`PasswordAuthentication`**, deploy fail2ban, rotate all 13 Spaces keys (eliminate orphaned keys, enforce least-privilege), enable backups on 4/7 droplets and snapshots on the 2 TB volume. Rotate the shared MongoDB Atlas credential and audit all 7 apps for hardcoded credentials.
WR36-03	WordPress Compromise Remediation	Remediate the active compromise on **`DO-LAMUSICA-WP`**: remove 8+ obfuscated PHP webshells from **`sbsmultisite`** uploads, secure **`wp-config.php.bak`** and the 1.14 GB SQL dump, patch the SSH brute-force vector (111k attempts in 7 days), and conduct a full malware scan. Rebuild from clean backup if necessary.
WR36-04	Cost Optimization and Resize Execution	Execute the validated resize plan for extreme oversizing: downsize STIMPY ($1,056/mo at 1% CPU) and REN ($806.40/mo at 0.2% CPU) based on 14 days of DO Insights telemetry (Aug 1024). Validate the projected saving of $1,750–1,850/mo (~$21,000/yr) with post-resize monitoring. Document the resize decision with rollback procedures.

4 Decisions of Record

DoR-1—Read-Only Audit Mode

Date: August 24, 2026

The entire LaMusica/SBS infrastructure security audit was conducted in strict read-only mode. No remediation actions were executed on production systems during the audit week. All findings were documented with evidence and delivered as reports, with remediation plans drafted but held for explicit user approval before execution. This

decision preserves system stability while ensuring all findings are auditable and reversible.

DoR-2—Immediate Credential Rotation Priority

Date: August 25, 2026

The plaintext MongoDB Atlas credential shared across 7 apps on REN and STIMPY, combined with plaintext AWS, Elastic, and Firebase Admin secrets committed to Git on HITZMAKER, constitutes a P0 security incident. The shared credential must be rotated immediately — before any other remediation — to prevent lateral movement. The rotation procedure must include: (1) generate new credential, (2) update all 7 app configs, (3) verify connectivity, (4) revoke old credential, (5) audit Git history for the old secret and rotate if exposed. The DO account 2FA codes in plaintext on the workstation must also be regenerated and stored in a password manager.

DoR-3—Payments API Authentication Before Any Other Remediation

Date: August 28, 2026

The unauthenticated **`GET /api/transactions/client`** endpoint on **`payments.spanishbroadcasting.com`** is an active data breach exposing customer PII (email, phone, address, bcrypt hashes, masked cards, expiration dates, Converge tokens) with a reproducible 30-second **`curl`** PoC. This vulnerability takes absolute priority over all other remediation work. The endpoint must be authenticated (OAuth2/API key + session validation) before the 3-day plan proceeds to Phase 2. The unauthenticated DoS vector (search **`?q=gmail`** 503) must be rate-limited simultaneously. No other infrastructure work may proceed until this endpoint is secured.

DoR-4—Canonical sbsdash Deployment Pipeline for Static Sites

Date: August 20, 2026

All static site deployments to SBS infrastructure shall follow the canonical pipeline: (1) clone/mirror from upstream source, (2) diff against previous version parsing **`const DATA`** JSON, (3) remove third-party injected scripts (e.g., **`sdk-seed.js`**), (4) obtain user confirmation, (5) rsync to **`/var/www/<domain>`** with **`--rsync-path="sudo rsync"`**, (6) add Caddy block, (7) copy favicon from **`ceo.sbsdash.com`**, (8) **`caddy validate + reload`**, (9) execute 10-point verification checklist (md5 integrity, 0 external refs, 0 console errors, DOM search, watermark, screenshot). This pipeline was validated on **`orgchart.sbsdash.com`** and **`hr-report1.sbsdash.com`**.

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-0034—Weekly Status Report — Week 34 (LHN-8005)

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

• auditoria-digitalocean.md—DigitalOcean Console Audit (LaMusica Team account)

• reportes/auditoria-do-ren-2026-08-25.{html,pdf}—REN droplet audit (ES/EN)

• reportes/auditoria-do-stimpy-2026-08-25.{html,pdf}—STIMPY droplet audit (ES/EN)

• reportes/auditoria-ubuntu-c-8-nyc1-2026-08-25.{html,pdf}—ubuntu-c-8 droplet audit (ES/EN)

• report-2026-08-26/—Elavon payments audit, remediation plan, and management brief (ES/EN, MD+HTML+PDF)

• reportes/poc-exposicion-api-pagos-2026-08-28.md—Live PoC: unauthenticated payments API exposure

• report-2026-08-28/—Buckets audit and databases audit (ES/EN, HTML+PDF)

• report-do-{lamusica-wp,hitzmaker,commercial-free-station,lamusica-wave}-2026-08-28/—19 reports per server + consolidated ES/EN PDF

• pdfs-reports-2026-08-28/{ES,EN}/—14 final per-server PDFs (7 servers × ES/EN)

6 Change Register

Entry	Date	Change
CR-01	August 28, 2026	Initial issue — no prior edits.