Security Audit — 026 "Installer Self-Breach + Skin Attack Surface"

Date: 2026-06-18 **Auditor:** Cowork session (Claude, Opus 4.8), for Sean **Severity:** High (availability / fleet lockout) + Medium (attack surface) **Status:** Remediated this session. Two cleanup/hardening items remain (see §6).

1. Summary

A fresh SnapSmack install locked itself out of admin on first login via false SMACKBACK breaches, fleet-wide. Two independent causes, same integrity-monitor surface, plus a separate installer over-install that needlessly widened attack surface. All remediated; residual hardening flagged.

2. Finding A — installer/setup self-delete → false MISSING breach (High)

`install.php` and `setup.php` are present on disk at install, get baselined by SMACKBACK, then self-delete (`@unlink(__FILE__)`). The next integrity scan sees them gone → **MISSING → LOCKOUT** on every fresh install. Normal users cannot self-recover (VAX is operator-only).

Remediated — exclude both filenames from monitoring in all three paths (they ship in the zip, but are never recorded in the integrity manifest): - `core/smackback.php` → `smackback_should_monitor()` - `smack-central/sc-release.php` → smackback manifest builder - `tools/_build/build-release.php` → `smackback_build_should_monitor()`

The earlier handoff documented this fix but it had never been applied, and it missed `sc-release.php` (the packager actually shipped from). Now closed in all three.

3. Finding B — install.php regenerates constants.php (drift) → false "truncated" (High)

`install.php` regenerated `core/constants.php` from a hardcoded string template (main flow ~1199, restore fallback ~1677). That template had drifted from canonical: wrong codename, reordered blocks, and **no EOF marker**. SMACKBACK baselines `constants.php` from the *release* file (which has the marker); the install-written file's last line differs → classified **"truncated"** on first login → breach, every fresh install.

The template's only dynamic value, `SNAPSMACK_TABLE_PREFIX`, is **dead** (zero read-sites in the codebase; all queries hardcode `snap_`), so regeneration served no purpose.

Remediated — regeneration disabled on both paths; the shipped canonical `constants.php` stands. (Dead template strings left in place, flagged for cleanup — see §6.)

4. Finding C — installer over-installs skins (Medium, attack surface)

`projects/snapsmack-ca/install-manifest.php` returned **every** registry skin whose `modes[]` matched the install mode; `install.php` then downloaded/extracted all of them. Result: unused skins land on every install — needless attack surface and unconsented shared-host disk use. This is how AURORA auto-installed fleet-wide on GRAMOFSMACK boxes.

Remediated — the manifest now returns only the mode's **default** skin (+ required `mobile_only` infrastructure). Optional skins install on demand from the in-CMS gallery. Ties to prior audits 020 / 021 (hub-spoke attack surface).

5. Posture notes (not vulnerabilities)

- **Hub→spoke email-identity push.** The multisite settings-push allowlist (`smack-push-it.php` `$push_group_keys['email']` **and** `core/multisite-api.php` `$allowed_keys` — both required) now carries `admin_email`, `email_from`, `email_from_name` (was `site_email` only), gated by `hub_controls_email`. Identity strings only — **no secrets distributed**.

- **2FA trust-device checkbox.** Rendering fix only (`smack-2fa-verify.php`): the checkbox was collapsed invisible by the global input reset. The trust mechanism (`ss_totp_trust` cookie + `snap_totp_devices`) is **unchanged** — no weakening, no policy change.

5b. Pimpotron / KIOSK engine removed (attack-surface reduction)

The cut KIOSK skin's Pimpotron engine sat orphaned in the tree: a **live admin page** (`smack-pimpotron.php`) and an **HTTP endpoint** (`pimpotron-payload.php`), plus engine JS/CSS, a manifest entry, an admin-nav link, and two DB tables — unreachable by design but still live, executable code = needless attack surface. Removed in 0.7.267: the four files deleted, `smack-pimpotron` manifest entry dropped, nav unhooked in `core/sidebar.php`, and tables dropped (`migrations/migrate-drop-pimpotron.sql` + canonical removal so schema-sync won't recreate them). The one reusable piece — a standalone Matrix-rain canvas class — was salvaged into a clean library engine `assets/js/ss-engine-matrix-rain.js` (`smack-matrix-rain`).

6. Residual / follow-up

1. **Dead install templates** — `$constants_php` / `$const_php` strings remain in `install.php` (no longer written). Excise in a cleanup commit.
2. **Updater version-write hardening** — `core/updater.php` ~1271 rewrites `constants.php` non-atomically and unguarded against a null `preg_replace`. Latent truncation risk; harden with atomic temp+rename and a post-write marker check. (Not the cause of this incident.)
3. **Planned SMTP/Brevo key push** (spec `_spec/smtp-mailer-spec-v0.1.md`, not built) WILL distribute a live secret to every spoke. Decided: one shared key. Re-evaluate per-spoke keys if blast radius becomes a concern (Brevo supports multiple SMTP keys).